

**PCT**WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau

## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification 6 :</b> <b>H04L 9/28</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 98/10562</b> <b>(43) International Publication Date:</b> 12 March 1998 (12.03.98)
<b>(21) International Application Number:</b> PCT/US97/15869 <b>(22) International Filing Date:</b> 9 September 1997 (09.09.97)  <b>(30) Priority Data:</b> 08/711,770 9 September 1996 (09.09.96) US  <b>(71)(72) Applicants and Inventors:</b> ANDERSON, Robert [US/US]; 1501 Barton Springs Road #214, Austin, TX 78704 (US). SCHULTZ, George, R. [US/US]; 513 Greenridge, Coppel, TX 75019 (US). HEPTIG, John, P. [US/US]; 7000 Treehaven, Fort Worth, TX 76117 (US).  <b>(74) Agent:</b> SCHULTZ, George, R.; Strasburger & Price, L.L.P., Suite 4300, 901 Main Street, Dallas, TX 75202 (US).		<b>(81) Designated States:</b> AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).  <b>Published</b> <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
<b>(54) Title:</b> ELECTRONIC ENCRYPTION DEVICE AND METHOD  <b>(57) Abstract</b>  A device and method are provided using a split processor based architecture to provide physical security of critical information by implementing a required protocol before releasing critical information. The critical information is used as a key to a cryptographic algorithm. A chaotic cryptographic algorithm is also provided including a defined key space employing six parameters of a Lorenzian system of equations.		

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KP	Democratic People's Republic of Korea	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KR	Republic of Korea	PL	Poland		
CM	Cameroon	KZ	Kazakhstan	PT	Portugal		
CN	China	LC	Saint Lucia	RO	Romania		
CU	Cuba	LI	Liechtenstein	RU	Russian Federation		
CZ	Czech Republic	LK	Sri Lanka	SD	Sudan		
DE	Germany	LR	Liberia	SE	Sweden		
DK	Denmark			SG	Singapore		
EE	Estonia						

## **ELECTRONIC ENCRYPTION DEVICE AND METHOD**

### **FIELD OF THE INVENTION**

The present invention relates generally to cryptographic data transmission  
5 and storage systems and more specifically, to microprocessor implemented  
cryptographic systems based on chaos theory.

- 2 -

**BACKGROUND OF THE INVENTION**

Message encryption has become increasingly necessary to maintain data privacy and integrity when transmitting messages over a computer network. Industry's reliance on computers and data transmission over networks has led to a  
5 substantial increase in the use of encryption systems to safeguard messages or data from unauthorized access. Modern encryption systems must account for not only cryptographic security, but physical security of the implementing hardware.

Encryption is the process of transforming a message into a form that is meaningless to everyone except the intended receiver. Cryptography is the science  
10 of making this transformation as intricate as possible, so that reversing it without certain key information is difficult, if not impossible.

Encryption algorithms must be invertible transformations so that encrypted messages can be decrypted. All transformations using the encryption algorithm are referred to generally as a "family" of transformations. Within the family of  
15 transformations, modern encryption systems use a key or seed which is a parameter which selects a particular transformation from the family of transformations. An important property of encryption algorithms is that unique keys will define unique encrypted messages or ciphertext.

A cryptosystem can be defined as an encryption algorithm, a decryption  
20 algorithm and a specific key which produces an unique invertible transformation using the given algorithm. Ideally, a cryptosystem uses the key and the algorithm

- 3 -

to produce a flat distribution for all properties of the message to be encrypted, hiding all natural redundancies of the language that make up the message. It should appear to the attacker that the message represents random information.

The security of a cryptosystem is directly related to the uncertainty of the  
5 attacker in determining the keys used to encrypt the message. Perfect security can be assured if the key is a string of truly random numbers and is as long as the message being encrypted. Such perfect security is known as a "one time pad" if the key is discarded after a single use.

A system is said to be computationally secure if the task of determining the  
10 key is computationally infeasible or intractable. A perfectly secure system is useful because the attacker does not have enough information from the ciphertext to determine the key. On the other hand, computationally secure systems are also useful because while the attacker has enough information in the ciphertext to determine the key, he does not have enough time to complete the task.

15       Computationally secure systems are rated by their resistance to three types of attack, "ciphertext only attack," "known plain text attack," and "chosen plain text attack." In each type of attack, the attacker is given the encryption and decryption algorithms and with this information attempts to decrypt the message. In the ciphertext only attack, the attacker is also given the encrypted message to  
20 examine. Any system failing this attack is considered totally insecure. In a known plain text attack, the attacker is given the algorithm, the original message and its

- 4 -

encrypted form. Cryptosystems which survive this attack are considered reasonably secure. A chosen plain text attack gives the attacker the algorithm, and the ability to encrypt and decrypt any message chosen. Cryptosystems which survive this attack are considered very secure.

- 5        Cryptographically, several encryption schemes are in wide use today, but each is unsatisfactory for several reasons.

      The digital encryption system, or DES as it commonly called, has been widely used by industry and the government since 1977. The DES system uses a 56 bit key to encrypt 64 bit data words through a lengthy process of  
10 transformations and substitutions. The computation time to transverse the transformations required to encrypt a large message or data file is substantial; therefore, for modern real time encryption applications, DES has fallen out of favor. The DES system has also been substantially challenged with modern super computers and is no longer approved for encrypting government messages.

- 15        The main disadvantage to the DES encryption system is that it is slow. The complex transformations used by DES require lengthy software programs to be implemented. Additionally, as the length of the message increases, the time to encrypt it under the DES standard grows linearly. Obviously, this limitation is undesirable in an cryptographic system. Dedicated circuits are available which are  
20 faster, but so far, they are prohibitly expensive. A second problem with the DES

- 5 -

encryption algorithm is that it provides no description of physical security with respect to the encryption key. Therefore, if the physical security of the key is compromised, the robustness the DES encryption algorithm is no protection. Another disadvantage of DES is that it leaves a signature in the encrypted file  
5 sufficient to identify that the DES algorithm has been used.

The Rivest-Shamir-Adelman (RSA) algorithm is also in wide use. It relies on the receiver giving the sender a "public key" and the encryption algorithm. The sender encrypts the message and sends it to the receiver using the public key and the algorithm. The receiver then can decode the message using a "private key."  
10 Only the intended receiver can decode the encrypted message.

The RSA algorithm is asymmetrical, which means that a different algorithm must be used for encrypting and decrypting messages. It uses keys of between 150 and 200 digits long, which is of considerable length. To invoke the algorithm, RSA requires calculation of a private key derived from the least common multiple  
15 of two large prime numbers. The difficulty in breaking and thus security of the RSA cryptosystem lies in determining the two prime numbers. This is an example of an intractable but soluble problem.

The main disadvantage of the RSA cryptosystem is that its security relies on the determination of two large prime numbers. As available computer speeds  
20 increase, the determination of these two prime numbers will become faster. Moreover, there is substantial mathematical research ongoing to determine new

- 6 -

prime number factoring algorithms. Therefore the security of the RSA cryptosystem is steadily and predictably decreasing most recently the key has been broken in as little as eight (8) months. Another disadvantage is that the RSA encryption system is very slow when implemented in software. Additionally, as  
5 the length of the encrypted message increases, the encryption time also increases drastically. As with DES, RSA can leave an encryption signature behind in the encrypted file which allows the encrypting algorithm to be identified. Another problem is that the RSA cryptosystem does not address physical security of the required keys.

10 Chaos theory has been suggested as a basis for cryptosystems. Chaos theory is based on simple deterministic systems that demonstrate random behavior. Some examples of natural phenomenon exhibiting chaotic behavior include atmospheric weather and turbulent water flow. Uncertainties in information about the system, that is errors, become magnified by the nonlinearity of the equations  
15 in the system, resulting in unpredictability of the system after a very short time. Some chaotic systems, like the Lorenzian system, are absolutely deterministic given an acceptable set of initial conditions. For the same initial conditions, the system produces the same results. So, even if the results are random, they are repeatable.

United States Patent No. 5,291,555, to Cuomo and Oppenheim discloses  
20 an analog electrical circuit which utilizes a system of Lorenz equations which exhibit chaotic behavior. In implementing these equations, a chaotic driver signal



- 7 -

$u_i$  is fed into subsystems synchronizing two additional signals  $v$  and  $w$ . Additionally,  $u_i$  is summed with a data signal  $m_i$ . The driver signal  $u_i$  is only slightly perturbed by summing with the message  $m_i$  and therefore masks the message  $m_i$ . The resulting encrypted signal,  $c_i$  is transmitted to the receiving station that uses  $c_i$  to synchronize the receiver's subsystems to recreate the original driver signal  $u_i$ . This driver signal is then subtracted from  $c_i$ , with the results being the original message  $m_i$ .

Cuomo and Oppenheim have also disclosed a digital encoding methodology (See Cuomo, Oppenheim, and Strogatz, Synchronization of Lorenz Based Chaotic Circuits with Applications to Communications, IEEE Transactions on Circuits and Systems - II, *Analog and Digital Signal Processing* 40, 10 (October 1993) 626-633; Also see Cuomo and Oppenheim, Circuit Implementation of Synchronized Chaos with Applications to Communications, Physical Letter 71, 1, July 5, 1993, pp. 65-68) that modifies the subsystem of  $w_i$  by modifying a constant  $b$  by the message stream  $m_i$ . The receiver would recognize digital 1's from 0's by the error induced by comparison from a nonencoded driver's signal  $u_i$ .

Both Cuomo and Oppenheim disclosures require that identical electrical components be used in the sending and receiving systems. This is a major drawback for a cryptosystem because of the difficulty in such construction on a commercial scale. Additionally, both disclosures are slow because they require a great deal of time to synchronize the receiver's components to the transmitter's

- 8 -

components; this is especially a problem with the digital application. An additional drawback of the Cuomo and Oppenheim disclosures is that each must use a narrow defined set of "tuning parameters" for each equation, which must be identical in both the transmitter and receiving circuits or digital applications.

5           A second digital application of chaos theory is disclosed by United States Patent No. 5,048,068 to Bianco and Reed. Bianco discloses the use of a single nonlinear logistic difference equation:

$$x_{n+1} = \mu x_n(1-x_n)$$

where  $\mu$  is a tuning parameter and  $x_n$  is a randomly selected number which serves  
10 as a key. In this invention, the key is multiplied by a fixed tuning parameter  $\mu$ . The resulting value is then iterated in the logistic difference equation to arrive at a chaotic stream of numbers. This chaotic stream of numbers is then compared with a range and a centerpoint. If the iterated results are in the top of the range, they are assigned a digital 1, if they are in the lower half of the range, they are  
15 assigned a digital zero. A domain transformation results, resulting in a random string of 1's and 0's. The stream of 1's and 0's is then added to a binary message to produce an encrypted message.

The Bianco system has several problems. First, it is slow. The logistic difference equation produces a random set of numbers. The numbers are more  
20 likely than not outside the predetermined range as required by the disclosure. If the number produced by the equation is outside the range, the equation must be

- 9 -

reiterated to produce another number. This process must repeat until the equation produces a number within the given range. Sometimes this can require many cycles before a useable number is generated. Second, the allowable keyspace for the logistic equation is very small, allowing brute force or iterative attacks to become possible. Third, no provision is made for assuring that the same key is not used repeatedly. Considering the small allowable keyspace, the same key must be used a number of times. The more often the same key is used, the more the cryptosystem becomes venerable to a chosen plaintext attack, thereby reducing its security. Fourth, no physical security is provided for the key required by the system. Therefore, like the DES and RSA encryption standards, no suggestion is given on how to maintain physical security of the key. If an attacker has the key, the Bianco system is useless to protect information.

- 10 -

SUMMARY OF THE INVENTION

The present invention provides a device and method which meets the needs of both physical and cryptographic security for cryptographic system. Physical security is provided by a split microprocessor based architecture. The architecture provides physical security of the key by implementing a required protocol before releasing critical information used by the cryptographic algorithm. In the preferred embodiment, this protocol includes the fragmentation of the protocol into three discreet storage areas. Each of the fragments is required in the protocol before key information is released. The physical security provided by the split processor architecture, and the fragmentation of required key information makes physical protection of the key virtually absolute.

The present invention further provides for cryptographic security by an improved digital implementation of the Lorenzian system of chaotic equations. The preferred embodiment of the invention provides that six parameters in these three Lorenz equations be chosen as a cryptographic key. A seventh parameter, "iterate sum", is also provided for which assures the uniqueness of each encrypted message. The improved digital implementation provides encrypted files which leave no statistical signature behind which would enable an attacker to determine which algorithm was used to encrypt the file. The digital application of the Lorenz system of equations as a cryptosystem virtually guarantees messages encrypted using the present invention will be invincible to chosen plain text attacks, making

- 11 -

it an extremely secure cryptosystem. Also, the improved implementation of the Lorenz system provides a robust cryptosystem without the need for domain transformations or repetitive iterative cycle times.

The invention further provides for a predefinition of a valid key space for  
5 the cryptographic algorithm. The valid keyspace allows iterative checking of random keys to be eliminated which substantially increases the speed of the encryption algorithm. The defined keyspace also avoids the need to define a new key for each application, and assures it has not been used previously.

The invention further provides for a keyspace which is sufficiently large to  
10 frustrate brute force attacks. That is simply trying each combination of keys possible until the encrypted message is discovered. The combination of the software and hardware provided ensures that such an attack will take over 5.8 billion years to complete successfully.

The advantages of the present invention can be applied to virtually any type  
15 of binary data transmission or storage. The most common practical application is the protection of data stored and transmitted on the Internet; however, the invention lends itself well to any other type of security need where binary data is transmitted or stored. The invention is especially well suited to applications where real time encryption and decryption of data is required such as digital cellular telephones or  
20 wireless data transmission networks.

- 12 -

### **BRIEF DESCRIPTION OF THE DRAWINGS**

Figure 1 shows a three dimensional plot of the results of the Lorenz equations disclosed iterated ten thousand times.

Figure 2 shows a plot of the value of the fourth byte of the z stream versus  
5 iteration number for ten thousand iterations of the disclosed equations.

Figure 3 shows a spectral distribution across a possible space of 0-255 integer values of the byte value versus the frequency of occurrence.

Figure 4 shows the disclosed cryptographic system response spiralling into a single x,y,z point.

10 Figure 5 shows the disclosed cryptographic system response settling into a single a predictable orbit.

Figure 6a shows an unencrypted spectral distribution of a *Microsoft Word* document file.

Figure 6b shows the spectral distribution of a *Microsoft Word* document file  
15 after being encrypted with the DES encryption standard.

Figure 6c shows the spectral distribution of a *Microsoft Word* document file after being encrypted with the RSA encryption standard.

Figure 6d shows the spectral distribution of a *Microsoft Word* document file after being encrypted with the cryptosystem defined by the preferred embodiment  
20 of the present invention.

Figure 7 shows the architecture of the preferred embodiment.

- 13 -

Figure 8a is a graphic representation of a memory model of the slave processor as disclosed configured to act as an "user class" token.

Figure 8b is a graphic representation of a memory model of the slave processor as disclosed configured to act as an "super user" token.

5        Figure 8c is a graphic representation of a memory model of the slave processor as disclosed configured to act as an "factory" token.

Figure 9 shows a flow chart of the program employed by the preferred embodiment to gain access to the initial conditions stored in the disclosed slaved processor.

10        Figure 10 shows a flow chart of the software executed by the preferred embodiment to verify protocol.

Figure 11 shows a flow chart of the software executed by the preferred embodiment to encrypt data.

15        Figure 12 shows a flow chart of the software executed by the preferred embodiment to decrypt data.

Figure 13 shows a flow chart of the software executed by the preferred embodiment to preprogram the disclosed slave processor.

Figure 14 shows a flow chart of the software executed by the preferred embodiment to program the disclosed slave processor by a user.

20        Figure 15 shows a flow chart of a second embodiment of the software used by the invention to encrypt data.

- 14 -

Figure 16 shows a flow chart of a second embodiment of the software used by the invention to decrypt data.



- 15 -

**DETAILED DESCRIPTION OF THE INVENTION**

The preferred embodiment of the invention employs an encryption algorithm which is a set of nonlinear equations developed by Edward Lorenz of MIT, 1963, from research into predicting atmospheric fluctuations. A reduced set  
5 of these equations is:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rx - y - xz \\z' &= bz + xy\end{aligned}$$

where the results  $x'$ ,  $y'$  and  $z'$  are derived by iterating the initial conditions  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $b$  and  $r$ . An iteration results when the results  $x'$ ,  $y'$  and  $z'$  are substituted into the equations for  $x$ ,  $y$  and  $z$ , to arrive at new results.

10 The Lorenz system is a simple deterministic system exhibiting random behavior when iterated with appropriate initial conditions. A three dimensional plot of the Lorenz equations iterated 10,000 times is shown as Fig. 1. A fundamental tenant of chaos theory is that behavior of the system is predictable in the short term but totally unpredictable in the long term. Therefore, the system can  
15 act as a random number generator with which to encrypt a message, in effect, a stream cipher algorithm. In the preferred embodiment, the cryptographic "key" is a unique set of initial conditions used to start the iteration process. This consists of three static variables  $\sigma$ ,  $r$  and  $b$  and three dynamic variables  $x$ ,  $y$  and  $z$ . Because encryption and decryption of the system is accomplished using the same algorithm,  
20 the preferred embodiment of the present invention is a symmetric encryption

- 16 -

algorithm and requires the use of the same key to encrypt and then decrypt a message.

For absolute security, the message to be encrypted must be encrypted with a truly random stream of encrypting bytes such a random stream is produced by the equations disclosed. The stream is used to encrypt one byte of the message at a time and therefore achieves the objective of a one time pad and assures that the message space and the encrypting space are of equal length and cardinality. Because the random stream is used only once, the ciphertext produced by the present invention is truly unbreakable.

One advantage of the system of Lorenz equations employed by the current invention is the production of three nearly random streams of numbers to be used to derive encrypting bytes,  $x'$ ,  $y'$  and  $z'$ . For example, if the Lorenz equations are iterated, preserving fifteen significant figures, Fig. 2 shows the plot of the value of the fourth byte of the Z stream versus iteration number when the equations are iterated 10,000 times using a set of valid initial conditions. Fig. 3 shows a spectral distribution across a possible space of 0-255 integer values of the byte value versus the frequency of occurrence. The spectrum shows that the values are randomly distributed across the potential of byte values, demonstrating that this stream has roughly an equal probability of being anything from 0-255 in value. Different initial conditions chosen from a valid key space can change the spectrum from uniform to more erratic in appearance. However, virtually any byte chosen from

- 17 -

any of the iterate streams will produce nearly random results.

The present invention uses the initial conditions for the Lorenzian system given as the key. The initial conditions consist of the three dynamic variables  $x$ ,  $y$  and  $z$  as well as the three static variables  $\sigma$ ,  $r$  and  $b$ . The variables create a six  
5 dimensional key space that defines all possible valid keys which can be used in the cryptographic system.

The initial conditions making up the key space cannot be random but must be chosen from the limited number in order to generate satisfactory encryption streams. Depending on the initial conditions, the Lorenzian system can respond  
10 in one of four ways, only one of which is satisfactory. First, the system can "blow up"; that is, the  $x'$ ,  $y'$  and  $z'$  values very quickly go to positive or negative infinity. This response is useless for a cryptographic system because the encrypting cipher quickly becomes stable at one value. In a digital application, the result is that the dynamic variables will quickly generate a floating point error once the  
15 maximum value exceeds the maximum word size. Second, as shown in Fig. 4, the system can spiral into a single  $x$ ,  $y$ ,  $z$  point and then stabilize there. This is obviously undesirable for encryption because a repetitive byte is far from random, and therefore offers no encryption capability. A third response, as shown in Fig. 5, is demonstrated where the system stabilizes in a predictable orbit. A long range  
20 periodicity is evident which is also useless for encryption because of its repeatability. The fourth possible response is a chaotic Lorenzian system with two attractors and

- 18 -

otherwise random results, as shown in Fig. 1. This type of result is ideal for a cryptographic system. However, it is possible only when a specific set of initial conditions are satisfied.

The following ranges of initial conditions are used by the preferred  
5 embodiment to achieve a satisfactory Lorenzian system:

Dynamic Variables

Static Variables

x about -30 to about +50, excluding 0

$\sigma$  about .006 - about .028

y about -30 to about +50, excluding 0

r about 24 - about 40

z about -30 to about +50, excluding 0

b about 1 - about 8

10 These ranges define the valid key space for the preferred embodiment of the present invention. The ranges are approximate and it should be understood that different implementations or equations may require different ranges to achieve a satisfactory chaotic system for encryption and decryption. A "key" is a unique set of each of the above parameters.

15 The number of keys provided by the present invention is extremely large. The potential number of different keys is defined by the ranges of the variables which make up the key space. Chaotic systems are extremely sensitive to initial conditions. A change in the 15th significant digit of any one variable in the key space is sufficient to generate a different random stream after a small number of  
20 iterations. Therefore, the number of possible keys in the key space of the present invention is determined by the product of the ranges of the six variables in the key

- 19 -

space divided by the minimum increment ( $1 \times 10^{-14}$ ) or approximately  $1.4 \times 10^{96}$  different keys. This represents a sufficiently large key space to render brute force attacks infeasible.

As an overview, the preferred embodiment consists of a properly  
5 programmed microprocessor and a removable, electrically active token. In order to encrypt a data file, three pieces of information must be present, a personal identification number (PIN) (memorized by the user and entered by a keyboard), a cryptographic key serial number (stored in a memory partition in the removable token) and the machine password (stored in a separate implementing processor).  
10 When the user wishes to encrypt a file, he attaches the token to the implementing processor via a connector and invokes the "encrypt" routine stored in the implementing processor.

The processor then combines the PIN, serial number and the machine password to compute a read password. The read password is then transmitted to  
15 the token which returns a preselected set of initial conditions stored in its memory.

In a first embodiment, encrypting and decrypting is started a certain predetermined distance down the iterate streams. A pseudo random number is chosen to indicate how many iterations to run before beginning decryption. This number is then stored in the encrypted file as a header.

20 The implementing processor substitutes the initial conditions into the Lorenz equations, iterates them the predefined number of times. At this point, the

- 20 -

implementing processor begins encrypting data with the iterate streams at this point, by xoring the data with the results of the Lorenz equations, a byte at a time. The encrypted data is then stored or transmitted. Decryption is essentially the mathematical reverse of this process, using the same token. However, the "file  
5 header" is read from the encrypted file and used to determine how many times to iterate the equations before beginning decryption.

In a second embodiment, the Lorenz equations, once initialized are allowed to iterate infinitely without repeating from the first set of initial conditions each time. This is accomplished as follows: On encryption of the first data file, the  
10 implementing processor begins at the first set of initial conditions, encrypting a message byte by byte. At the end of the first message file, the variables x, y and z are stored in a file or back in the token, for future use. Upon encrypting a second message, the implementing processor adopts the stored variables x,y and z to be inserted into the Lorenz equations. The implementing processor then begins  
15 encryption of the next message at this point.

The net result is that from message to message, the iterate stream from the first set of initial conditions continues infinitely, xoring one message after another with the continuing iterate stream. Decryption is essentially the mathematical reverse of this process.

20 An advantage of the second embodiment is that the initial x,y and z variables, after used once to generate the iterate streams, may be erased from

- 21 -

storage in the token, forever eliminating the possibility of discovery. In other words, after the iteration of the equations has begun, the original x,y and z initial conditions, or "seed" can be destroyed. Without this seed, the past behavior of the equations, and the ability to regenerate it is lost.

5       The preferred embodiment allows several tokens to be used with an implementing processor, and several implementing processors to be activated with a single (or multiple) token(s). It also allows the user to install new tokens to be used for additional users. The invention provides for three classes of tokens, each having different capabilities, and different information stored in their memory  
10       partitions. A "super user class" is allowed to encrypt and decrypt data, and install new "user" tokens; the "user class" can just encrypt and decrypt data; a "factory class" token is not allowed to encrypt or decrypt data or set up new user tokens, but does carry information necessary to the original installation of the entire cryptographic system.

15       In more detail, the preferred embodiment of the present invention is implemented using the architecture shown in Fig. 7. Fig. 7 shows an architecture  
20       comprised of a master processor 12 and a slave processor 14. In the preferred embodiment, master processor 12 is an *Intel pentium* processor as used in common personal computers running in a DOS based environment. Other operating systems  
20       such as Unix can also be used with equal success. Of course, other microprocessors such as the *Motorola 68000* family, the *Intel 8088* family, *Intel*

- 22 -

*ix86* family or *RISC* based microprocessors may be used with suitable results. Additionally, discrete logic circuits or custom processor designs can be used to implement the necessary functions required to implement the necessary software steps. The internal architecture of the *Intel pentium* processor is well known in the art and will not be described further here.

Each token in the preferred embodiment incorporates a slave processor 14, shown in Fig. 7. Slave processor 14 consists of a comparator 16, I/O control circuitry 18 and a memory area 20. Slave processor 14 in the preferred embodiment provides for at least three separate memory partitions in memory area 20, each one of which is set to variable levels of accessibility. At least two partitions can be set to require passwords or not. If the memory partition is configured to require a read password, read access to the partition is only allowed when the read password is given. Similarly, if configured to require a write password, write access to each of the partitions will only be granted if the write password is supplied. If configured not to require passwords, slave processor 14 will allow read or write access to the memory partitions without the necessity of receiving a password. A configuration password, also stored in slave processor 14 allows the user to reprogram the read and write passwords.

Slave processor 14 in the preferred embodiment is the *Xicor X76041* password access security supervisor chip available from Xicor Incorporated located in Malipitas, California. The *X76041* is a dedicated password access processor



- 23 -

containing four 128 x 8 bit *EEPROM* arrays. Access to each array can be controlled by three 64 bit programmable passwords, one for read operations, one for write operations and one for device configuration. As configured in the present invention, access to the memory 20 is only allowed after communication of a valid password protocol as will be described more fully later. Other processors can be substituted for the *X76041*, including the *Intel*, *Motorola* or other microprocessors, custom processors or discrete logic components which are capable of performing the software steps required.

Slave processor 14 is connected to master processor 12 through a serial interface on a simple two-wire bus. The bus signals are a clock input (SCL) 22 and a bidirectional data input and output line (SDA), 24. In the preferred embodiment, power is supplied through a separate power bus 26. Physically, slave processor 14 is housed in a separate plastic package which is detachable from master processor 12 through a standard four pin connector (not shown). The four pin connector provides connections for the SCL line 22, the SDA 24, and power and ground lines for power bus 26.

Architecture 10 also includes, inbound memory 28, outbound memory 30 and program memory 37. In the preferred embodiment, memories 28, 30 and 37 are hard storage such as a fixed disks or floppy disks. However, any equivalent storage device, such as optical medium, buffers or magnetic tape can also be used. Additionally, inbound memory 28 and outbound memory 30 can be replaced by

- 24 -

input/output (I/O) ports which are addressable by master processor 12 for real time receipt and transmission of data, respectively. This feature is useful in applications where encryption and decryption of data is necessary on a real time basis, without storage.

5           Architecture 10 also includes an I/O port 32, a machine password memory 34 and read only memory (ROM) 36. In the preferred embodiment, I/O port 32 has a standard PC keyboard. However, I/O port 32 can be any number of I/O devices such as key pads, magnetic card readers or optical scanners.

Machine password memory 34 in the preferred embodiment is a hard disk.  
10   However, memory 34 can also take other forms of non-volatile memory such as ROM or battery backed-up RAM, floppy disks or optical or tape storage. ROM 36 is provided in architecture 10 to allow booting of master processor 12. ROM 36 may also contain the necessary software routines to implement the invention which can be loaded at start-up of master processor 12 or vectored to locations in program  
15   memory 37 which contain the necessary routines which can be accessed at run time.

Inbound memory 28, I/O port 32, machine password memory 34, outbound memory 30, read only memory 36 and program memory 37 are all connected to master processor 12 via address bus 37 and data bus 40. Details of addressing  
20   modes and data transmission are well known in the art will not be further described.

- 25 -

Power supply 42 supplies operating voltage to both master processor 12 and slave processor 14 via power bus 44 and 26, respectively. The attributes of the power bus and supply are well known in the art and will not be further described.

To install the preferred embodiment of present invention, a user receives  
5 two new "factory" tokens and essential software routines on a portable disk. The user supplies necessary information such as the personal identification number and machine password which allows the installation routine to program "user" tokens and "super user" tokens. After being initially configured, the tokens are ready to be used to encrypt and decrypt data.

10 Figs. 8a, 8b and 8c are graphical representations of three memory models of slave processor 14. The first row of each model depicts the level of access allowed to the data stored in each memory partition. The second row depicts the password requirement for access to the data stored in each partition. The third row represents the data stored in each partition. The fourth row represents the address  
15 of each kilobyte of data stored. The rightmost column of each model represents the first kilobyte memory partition of the slave processor. The center column represents the second kilobyte memory partition. The leftmost column represents the memory partition allocated for storage of the chip control passwords.

More specifically, Fig. 8a is a graphic representation of a memory model  
20 of slave processor 14 configured to act as a "user" token. As can be seen, both the first 1096 bytes ("First k"), hex address 000 through 078, and the second 1096

- 26 -

bytes ("second k") hex address 080 through 0FF, are set to allow read access only, as shown at 80 and 81. The password requirement of the first k partition, shown at 82, is set not to require a read password for access to the information in the first partition. The password requirement of the second k partition is set to require a  
5 read password to allow read functions, shown at 83. In the data area of the first partition, the token serial number is stored. In the preferred embodiment, each token is individually serialized with an eight byte serial number shown at 84. The initial conditions for the Lorenz equations are stored in the second k memory partition shown at 85. Slave processor 14 also includes an access password  
10 memory shown as 86, 87 and 88. At memory location 86, the 8 byte read password is stored, the 8 byte write password is stored at location 87 and an 8 byte configuration password is stored at 88. Preferably, slave processor 14 does not allow any read access of memory locations 86, 87 and 88.

Fig. 8b is a graphic representation of a memory model of slave processor  
15 14 configured to act as a "super user" token. As can be seen, both the first k, the second k partitions are set to allow read access only, as shown at 95 and 96. The password requirement of the first k memory partition, shown at 97, is set not to require a read password for access to the information in the first partition. The password requirement of the second k memory partition is set to require a read  
20 password to allow read functions, as shown at 98. The "super user" token serial number is stored in the first k partition of memory at 99. At location 100 in the

- 27 -

second k memory partition, the initial conditions are stored along with the configuration password. The access password memory partition shown as 101, 102, and 103 holds respectively, a read password, a write password and a configuration password, each 8 bytes in length. It is necessary to store the  
5 configuration password at memory location 100 in addition to memory location 103, because memory location 103 is restricted. In order to configure other tokens, the configuration password, shown at 103, must be accessible. By storing the configuration password in memory location 100, it is available for programming new tokens.

10 Fig. 8c is a representation of a memory model of a slave processor 14 configured to act as a "factory" token. As can be seen, the first k and second k memory partitions are set to allow read access only, shown at 89 and 90. The password requirement of the first k memory partition, shown at 91 is set to not require a read password for access to the information in the first partition. The  
15 password requirement of the second k memory partition is also set not to require a read password to allow access, as shown at 92. At the data area of the first partition, the token serial number is stored, along with an original configuration password, set to "0000000", shown at 93. In the data area of the second partition, shown at 94, the initial conditions for the Lorenz equations are stored. The  
20 configuration password is stored in the tokens access password memory partition, 104, as "0000000". It is necessary to store the configuration password of the

- 28 -

factory token twice so that when the factory token is reprogrammed by the system user, it's access and function levels can be configured appropriately. Further description of the memory partitions and programming details of the X76041 are well known in the art and will not be further described here. The disclosure in

5 XICOR Application Note and Development System AN67.XK76, "Password Access Security Supervisor-4K-X76041-4x128x8 Bit", Pass<sup>TM</sup>E<sup>2</sup>, release date 6/1/95 is incorporated herein by reference.

In the preferred embodiment, each parameter of the initial conditions is required to be calculated to 14 significant figures. Parameters with resolution out

10 to 14 significant figures provide sufficient resolution to achieve the maximum number of keys available in the valid key space. To active 14 significant figures, each parameter must use at least eight bytes of memory. Each parameter is stored in standard *IEEE* format, with the left-most bit being the sign bit of the parameter, the second most significant bit being the sign bit of the exponent of the parameter,

15 the following seven most significant bits being the number of the exponent, and the following six most significant bytes forming the value of the parameter. Of course, other data structures can be used equally as well.

In order to gain access to the initial conditions stored in slave processor 14, the master processor 12 in the preferred embodiment executes the software routine

20 105 shown in Fig. 9. First, at step 106, master processor 12 sends slave processor 14 the appropriate command sequence telling slave processor 14 that a read

- 29 -

operation is requested, and an address in memory area 20 to read the serial number stored in the first memory partition, 84. All communication takes place serially over SDA line 24, moderated by a clock signal generated by master processor 12 and transmitted over SCL line 22. If an acknowledge signal is received from slave processor 14 at step 107 by master processor 12, then, master processor 12 reads the eight byte serial number via SDA line 24 and stores it in temporary memory, as shown at step 108. If no acknowledge signal is received at step 107, then master processor 12 repeats the send command step 106. This cycle repeats until an acknowledge is received by master processor 12 or time out condition is reached (not shown). Next, master processor 12 executes step 109 by polling I/O port 32, shown in Fig. 7. The user of the system responds by entering his personal identification number (PIN) which is communicated through I/O port 32 to master processor 12. At step 110, master processor 12 polls machine password memory 34 and receives the individual password assigned to it during installation of the system, which will be further described later. Master processor 12 then executes step 111 wherein the PIN, machine password and the serial number are XORED together to compute a read password; the read password is stored in temporary memory. At step 112, master processor 12 sends the command code for read, along with the address of the initial conditions stored in slave processor 14, in order to initiate a read of the initial conditions stored in the second k memory partition of slave processor 14, shown at 85 in Fig. 8. Master processor 12 then

- 30 -

waits at step 114 for an acknowledge signal to be received from slave processor 14. Upon receipt of the acknowledge signal at step 114, master processor 12 moves to step 116 and clocks out the eight byte read password on SDA line 24 at step 116. Master processor 12 then waits to receive an acknowledge signal from slave  
5 processor 14 indicating that the read password has been received and matches the access read password stored in slave processor 14. However, before slave processor 14 generates this acknowledge signal, it must execute a verification protocol to identify the read password sent by master processor 12.

The protocol verification routine is shown at Fig. 10. Slave processor 14  
10 is found in a hold state at 130. Upon receiving the read command, and the address of the data to be read at step 132, slave processor 14 responds by sending an acknowledge signal at step 133. If data is not properly received by slave processor 14, no acknowledge signal is sent, and slave processor returns to the hold state, 130. Assuming correct transmission of data and sending of the acknowledge signal  
15 in step 133, slave processor 14 moves to step 134 where it clocks in the read password from SDA Line 24. The read password is then compared, via comparator 16 of slave processor 14 to the read access password stored at password memory location 86 of slave process 14, shown in Fig. 8. If the read passwords match, then an acknowledge signal is sent from slave processor 14 to master  
20 processor 12 at step 140. If the passwords do not match, slave processor 14 waits ten milliseconds at step 138, and then returns to the hold state 130. Step 138 is



- 31 -

included to frustrate brute force electronic attacks, that is simply trying each read password until slave processor 14 allows access to the initial conditions. With a read password length of eight bytes and a wait state of ten milliseconds at step 138, it would take approximately 5.8 billion years to check each password possibility.

- 5 After sending the acknowledge signal, slave processor 14 then clocks out the initial conditions stored in second k memory partition 85 in Fig. 8.

Returning to Fig. 9, if no acknowledge is received, at step 118, master processor 12 reports an invalid access attempt at step 120. If a valid acknowledge signal is received at step 118, master processor 12 reads the initial conditions from  
10 slave processor 14 on SDA line 24 at step 122. Once master processor 12 has the initial conditions, it proceeds to step 124 where it can proceed to the encode or decode sequence shown at Figs. 11 and 12 or Figs. 15 and 16.

In one embodiment, master processor 12 encrypts data by executing the program depicted in Fig. 11. At step 150 master processor 12 generates a pseudo  
15 random number, 2 bytes in length, from any number of pseudo random functions available, and stores it in temporary memory. At step 152 master processor 12 executes routine 105, shown in Fig. 9, to obtain the initial conditions  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$  and  $b$ . At step 158, the pseudo random number derived in step 150 is written to the encrypted file as the first several bytes or as a file header. The pseudo random  
20 number generated is different for each file encrypted. It serves as an indicator how far down the iterate stream the processor is allowed to run before beginning the

- 32 -

actual encryption of data. Because each file is encrypted beginning at a different point down the iterate stream, each encrypted file is different, even if the files to be encrypted and the initial conditions are the same. This aspect of the current invention thereby frustrates chosen plain text attacks. As will be described later, 5 the pseudo random number is also used by the decryption sequence to indicate how long to iterate the Lorenz equations before beginning decryption.

The Lorenz equations are iterated at step 159. At step 160, master processor 12 polls inbound memory 28 to get a byte of the data file to be encrypted. At step 162, this byte of data is then XORED with a preselected byte 10 of the  $z'$  iterate stream.

The advantage of using an XOR operation is that it is a reversible operation. That is, a byte of data encrypted with a byte of the iterate stream may be decrypted by XORING the encrypted data with the same byte from the same iterate stream.

Of course, any byte of the  $x'$ ,  $y'$  or  $z'$  streams may be used as ciphertext. 15 Additionally, in an alternate embodiment (not shown) bytes from each of the  $x'$ ,  $y'$  and  $z'$  iterate streams are XORED together to create the ciphertext, one byte at a time.

At step 164, the encrypted message is written to a temporary file. At step 166, master processor 12 checks to determine if the last byte of data to be 20 encrypted has been read from inbound memory 28. If it has, the entire encrypted file is written to outbound memory 30 at step 168 and the encrypt sequence is

- 33 -

terminated at step 170; if not, master processor 12 returns to step 159 to reiterate the Lorenz equations.

In a second embodiment, master processor 12 encrypts data by executing the program depicted in Fig. 15. This embodiment, differs from the prior  
5 embodiment in that encryption begins at the first iteration of the Lorenz equations. Instead of beginning encryption a certain of distance down the streams, but restarting the streams upon each use of the encryption routine, the second embodiment never restarts the iterate streams, but rather allows them to continue uninterrupted, from one message to the next. Essentially, the encryption of each  
10 new message begins where the encryption of the prior message left off.

Referring to Fig. 15 at step 400, master processor 12 executes routine 105, shown in Fig. 9, to obtain the initial conditions  $x, y, z, \sigma, r$  and  $b$ . At step 402, master processor 12 checks an on board file, containing  $x_{(n+1)}, y_{(n+1)}$  and  $z_{(n+1)}$  from the prior encryption session. This file contains the last value of  $x_{(n+1)}, y_{(n+1)}$  and  
15  $z_{(n+1)}$  to be used to iterate the Lorenz equations. If the equations are being iterated for the first time, the values of  $x_{(n+1)}, y_{(n+1)}$  and  $z_{(n+1)}$  will be zero. In this event, at step 402, master processor 12 proceeds to step 406, where the Lorenz equations are iterated and new values for  $x_{(n+1)}, y_{(n+1)}$  and  $z_{(n+1)}$  are generated. If the program has been used previously, master processor 12 proceeds to step 404, and replaces  
20 the initial conditions  $x, y$  and  $z$  received at step 400 with the values of  $x_{(n+1)}, y_{(n+1)}$  and  $z_{(n+1)}$  stored in the file. Master processor 12 then proceeds to step 406 and

- 34 -

iterates the Lorenz equations beginning with the initial condition  $x_{(n+1)}$ ,  $y_{(n+1)}$ ,  $z_{(n+1)}$ ,  $\sigma$ ,  $r$  and  $b$ .

At step 408, master processor 12 polls inbound memory 28 to get a byte of the data file to be encrypted. At step 162, this byte of data is then xored with a preselected byte of the  $z'$  iterate stream to generate an "encrypt byte". At step 412 this encrypt byte is written to a temporary file.

At step 414, master processor 12 checks to determine if the last byte of data to be encrypted has been read. If not, it returns to step 406 where the Lorenz equations are iterated again to determine a new  $x_{(n+1)}$ ,  $y_{(n+1)}$  and  $z_{(n+1)}$ ; if the last byte of data has been read, master processor 12 writes the current  $x_{(n+1)}$ ,  $y_{(n+1)}$  and  $z_{(n+1)}$  values to a file at step 416 and ends the encryption routine at step 418.

The decryption routine of the first embodiment to decode encrypted messages, shown in Fig. 12, is similar but not identical to the encryption routine shown in Fig. 11. At step 190, master processor 12 polls inbound memory 28, which now holds an encrypted file, and reads the pseudo random number stored in the file header at step 158 of Fig. 11. At step 192, the processor then invokes the initial condition routine 105 to get the initial conditions stored in memory 20 of slave processor 14. At step 194, the initial conditions are substituted into the Lorenz equations and iterated the number of times indicated by the pseudo random number. Master processor 12 then proceeds to step 204, where it retrieves a byte of encrypted data from inbound memory 28 (now containing encrypted data). The

- 35 -

equations are iterated again at step 205 to get another byte of cipher text. At step 206, first byte of encrypted data is XORED with the  $z'$  iteration stream byte of cipher text. Step 206 results in decrypting the byte of encrypted data. The decrypted byte is then written to the outbound memory 30, at step 208. At step 5 210 the processor checks inbound memory 28 to determine if all data has been decrypted. If not, master processor 12 returns to step 204 to retrieve another byte of encrypted data from inbound memory 28 then the Lorenz equations are iterated again at step 212. If the last byte of data has been retrieved and decrypted at step 210, master processor 12 ends execution at step 214.

10       The decryption routine of the second embodiment to decode encryption messages, shown in Fig. 16, is similar to but not identical to the encryption routine shown in Fig. 15. The decryption routine of the second embodiment also keeps track of how many iterations down the iterate stream are required for each message, beginning decryption for each successive message at the iteration stream 15 termination point from the prior message. More specifically, at step 450, master processor 12 invokes initial condition routine 105 to obtain the initial conditions stored in memory partition 20 of slave processor 14. At step 152, the previous values of  $x_{(n+1)}$ ,  $y_{(n+1)}$  and  $z_{(n+1)}$  are retrieved and checked to see they are all zero. If they are, the program assumes that it is the first time decryption has been 20 requested and iterates the Lorenz equations to generate values of  $x_{(n+1)}$ ,  $y_{(n+1)}$  and  $z_{(n+1)}$ . If not, at step 454, master processor 12 replaces the initial conditions  $x, y$

- 36 -

and  $z$  retrieved at step 450 with the initial conditions  $x_{(n+1)}$ ,  $y_{(n+1)}$  and  $z_{(n+1)}$  retrieved from a file where they were stored at the end of the last decryption, and then proceeds to step 456 to iterate the Lorenz equations.

At step 458, master processor 12 polls inbound memory 28 to get a byte of the data file to be decrypted. At step 460, this data is xored with a byte of the  $z$  iterate stream to produce a decrypted byte. At step 462, this byte is written to a temporary file. Master processor then checks to see if the last byte of data has been decrypted at step 464. If it has not, the processor returns to step 456, to reiterate the Lorenz equations. If it is, processor moves to step 466 where the current values of  $x_{(n+1)}$ ,  $y_{(n+1)}$  and  $z_{(n+1)}$  are written to a file to be used as initial conditions to begin the next encryption. Execution terminates at step 468.

The preferred embodiment of the invention allows for several different slave processors to be used in conjunction with the same master processor, or different master processors. The slave processor is used as a "token" and is wholly portable from the master processor. Other tokens can be used equally well, such as magnetically encoded cards, bar codes or other memory storage devices. Additionally, in conditions where less stringent physical security is required, slave processor 14 can be incorporated as a nonremovable partition in master processor 12 or exclusively in software executed within master processor 12. In this case, the functions of slave processor 14 can be carried out from within master processor 12 itself, or can collapse into a simple password requirement.

- 37 -

In the preferred embodiment, each slave processor 14 is preprogrammed before it is received by the user. Preprogramming routine 220 is shown in Fig. 13. In order to preprogram each slave processor 14, master processor 12 proceeds sequentially through the valid key space, assigning each slave processor a unique  
5 set of initial conditions, and serial numbers. The assignment of initial conditions is not random, but is sequential to ensure complete usage of the valid key space. Additionally, the access configuration password may be set to all 0's for each token, so that it can be read and reprogrammed upon receipt by the user.

In more detail, at step 222, master processor 12 sets the initial values for  
10 the initial conditions as  $x = y = z = -30$ ,  $\sigma = .006$ ,  $r = 24$ , and  $b = 1$ . At steps 224, 226 and 228, master processor 12 increments the  $x$  parameter and checks to see if it is valid and within range. If it is, the other parameters of the initial conditions are assumed to be valid and master processor 12 moves to step 256 where the parameters are written to the slave processor 14 via SDA line 24. The  
15 new initial conditions then consist of the current incremented value of  $x$  and the initial values of  $y$ ,  $z$ ,  $\sigma$ ,  $r$  and  $b$ . If the  $x$  parameter is out of range, the processor moves to step 230, 232, and 234 where the  $y$  parameter is incremented, and checked to see if it is valid and within range. If it is, master processor 12 proceeds to step 256 where the new set of initial conditions is written to slave processor 14.  
20 The new initial conditions then consist of the current incremented value of  $y$ , the last valid value of  $x$  and the initial values of  $z$ ,  $\sigma$ ,  $r$  and  $b$ . If the  $y$  parameter is out

- 38 -

of range, Processor 12 moves to steps 236, 238 and 240 where the  $z$  parameter is incremented, and checked to see if it is valid and within range. If it is, a new set of initial conditions is written to the slave processor 14. The new initial conditions then consist of the current incremented value of  $z$ , the last valid value of  $x$ ,  $y$  and

5 the initial values of  $\sigma$ ,  $r$ ,  $b$ . If it is not, master processor 12 moves to steps 242 and 244 where the  $\sigma$  parameter is incremented and checked to see if it is within range. If it is, again the new set of initial conditions is written to the slave processor 14. The new initial conditions then consist of the last valid values of  $x$ ,  $y$ , and  $z$ , the current value of  $\sigma$  and the initial values of  $r$  and  $b$ . If it is not, master

10 processor 14 moves to steps 246 and 248 where the  $r$  parameter is incremented and checked to see if it is in range. If it is, a new set of initial conditions is written to the slave processor 14. The new initial conditions then consist of the current value of  $r$ , the last valid values of  $x$ ,  $y$ ,  $z$  and  $\sigma$  and the initial value of  $b$ . If it is not, master processor 14 moves to steps 250 and 252, where the  $b$  parameter is

15 incremented and checked to see if it is within range. If it is, the new set of initial conditions is written to the new slave processor 14. The new initial conditions then consist of the last valid value of  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$  and  $b$ . If it is not, at step 254 master processor 12 has reached the end of the valid key space whereupon no further valid initial conditions exist which will create a satisfactory Lorenz system.

20 Assuming that a valid set of initial conditions has been written to slave processor 14, master processor 12 moves to step 258 where it chooses a pseudo



- 39 -

random 8 byte integer as the slave processor's new serial number. At step 260, master processor 12 polls inbound memory 28, (which now holds a data file of previously used serial numbers and initial conditions), to determine if the serial number has been used previously. If it has, master processor 12 loops back to step 5 258 to pick a different 8 byte serial number. If it has not been used, master processor 12 moves to step 262 where it sets the configuration password of slave processor 14 to all zeros. At step 264, slave processor 14 is configured to allow access to the first and second k memory partitions without a read password. At step 266, master processor 12 writes the serial number and the configuration 10 password to the first k memory partition and the new initial conditions to the second k memory partition in slave processor 14. The routine concludes at step 268.

At this point, a "factory class" token containing the slave processor 14 has been programmed and allows free access to its memory, now containing the token 15 serial number, configuration password, and the initial conditions. However, before the new token can be used in the preferred embodiment, it must be set up as shown in Fig. 8a or 8b, thereby customizing slave processor 14 to include the new read password formed from the personal identification number, the machine password and the token serial number. This is accomplished through the set up routine as 20 shown in Fig. 14.

- 40 -

Moving to Fig. 14, at step 300, master processor 12 is connected to the "factory class" tokens as previously programmed, freely retrieving the token serial number, and the initial conditions stored in slave processor 14. At step 305, master processor 12 queries the user, through I/O port 32 to input if the installation  
5 is of a new system, receiving a yes or no answer. If the answer is no, master processor 12 skips to step 310. If the answer is yes, master processor 12 executes step 307 to get the configuration password and proceeds to step 310. At step 310, master processor then polls I/O port 32, to determine input his personal identification number. This number is stored in temporary memory. Once  
10 received, master processor 12 again queries I/O Port 32 to obtain an 8 byte machine password. In step 312, this machine password is stored in machine password memory 34. Moving to step 313, the serial number, the machine password, and the personal identification number are XORED together to derive the read password. At step 314, a pseudo random method is used to pick an 8 byte  
15 configuration password. At step 316 this new configuration password is sent to slave processor 14 and established as its new configuration password. At step 318, the new configuration password is used to send a command sequence to set up the function and access levels of the memory partitions of slave processor 14, as in Fig. 8a or 8b. In step 320, the new read password is sent to slave processor 14,  
20 to reside in memory slave processor 14 as shown in Fig. 8a or 8b. At step 322, the new initial conditions are written to the second k memory partition, as shown

- 41 -

in Fig. 8a to create a "user" token as shown in Fig. 8a, or, alternatively, the new initial conditions and the new configuration password are written to the second k memory partition as shown in Fig. 8b, to create a "super user" token. If the result of step 305 was no, master processor executes set up routine 324. In step 324  
5 master processor 12 writes the encryption routine shown in Fig. 11 or Fig. 15, the decryption routine shown in Fig. 12 or Fig. 16 and the set up routine shown in Fig. 14 to program memory 37, if the result of step 305 was yes, master processor skips to step 325. In step 325, master processor 12 writes serial number and configuration password to outbound memory 30 as a backup for future use. The  
10 routine then ends at step 326.

The effectiveness of the algorithm in altering the spectral distribution of a typical word processor document is illustrated in Figs. 6a through d. Fig. 6a shows an unencrypted spectral distribution of a *Microsoft Word* document file. Fig. 6b shows the file after being encrypted with the DES encryption standard. A  
15 notable DES signature is present through the repetitive peaks and valleys obvious throughout the encrypted file. Fig. 6c shows the same *Microsoft Word* document file encrypted using the RSA encryption standard. Again, the RSA system leaves a characteristic signature showing evidence of the original ASCII and blank characters being heavily weighted in the original spectrum. Fig. 6d shows the  
20 *Microsoft Word* document file encrypted using cryptosystem defined by the present invention. It can be seen if there is no information left the ciphertext that could be

- 42 -

used to reveal the methodology of encryption or the original message spectrum.

The speed of the encryption system in the present invention was also compared to the DES and RSA standards on a *pentium* personal computer. All three algorithms were implemented using *Turbo C* and a 1.3 megabyte file. The  
5 RSA implementation for the 200 digit key was extrapolated to two kilobytes per second. The DES implementation was measured at 33.9 kilobytes per second. The cryptosystem of the present invention was measured at 1,521 kilobytes per second. The present invention resulted in encryption 45 times faster than DES and 760 times faster than the RSA implementation.

Having described specific embodiments of the present invention, it will be understood that modifications thereof may be suggested to those skilled in the art, and it is intended to cover all such modifications as fall within the scope of the appended claims.

- 43 -

What is claimed:

1. A data encryption and decryption system comprising:
  - a. means for selecting a set of parameters from a predetermined valid parameter space;
  - b. means for inserting the parameters into chaotic equations of the form:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x'$ ,  $y'$  and  $z'$  are numeric results and  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$  and  $b$  are parameters;

- c. means for iterating the chaotic equations to derive  $x'$ ,  $y'$  and  $z'$  iterate streams;
  - d. means for deriving a cipher number from the iterate streams; and
  - e. means for xoring the cipher number with the data.

2. The system of claim 1, wherein the predetermined valid parameter space further comprises one parameter from each of the following ranges:

$x$  = about -30 to about 50, excluding 0  
 $y$  = about -30 to about 50, excluding 0  
 $z$  = about -30 to about 50, excluding 0  
 $\sigma$  = about .006 to about .028  
 $b$  = about 24 to about 40  
 $r$  = about 1 to about 8

- 44 -

3. The system of claim 1, further comprising:
  - a. means for iterating the chaotic equations a predetermined number of times; and
  - b. means for appending the predetermined number to encrypted data.
4. The system of Claim 1, further comprising:
  - a. means for storing parameters x, y and z; and
  - b. means for inserting the stored parameters into the chaotic equations.
5. The system of Claim 1, further comprising:
  - a. means for iterating the chaotic equations a predetermined number of times;
  - b. means for encoding the predetermined number; and
  - c. means for appending the encoded number to encrypted data.
6. A data encryption system comprising:
  - a. a predetermined set of valid initial conditions;
  - b. a protocol responsive memory programmed to store and allow access to the initial conditions in response to a protocol;
  - c. a processor connected to the protocol responsive memory, the processor programmed to:

- 45 -

- (1) execute the protocol;
- (2) receive and store the initial conditions returned by the protocol responsive memory;
- (3) insert the initial conditions into and iterate a set of chaotic equations to arrive at iterated results; and
- (4) create encrypted data by combining data with the iterated results.

5

7. The data encryption systems of Claim 6, further comprising a transmitter connected to the processor for transmitting the encrypted data.

8. The data encryption system of Claim 6, further comprising a second memory connected to the processor to store the encrypted data.

9. The system of Claim 6, wherein the set of chaotic equations are of the form:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rx - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x'$ ,  $y'$  and  $z'$  are iterated results of initial conditions  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$ , and  $b$ .

- 46 -

10. The system of claim 9, wherein the predetermined valid initial conditions are in the range:

5  
x = about -30 to about 50, excluding 0  
y = about -30 to about 50, excluding 0  
z = about -30 to about 50, excluding 0  
 $\sigma$  = about .006 to about .028  
b = about 24 to about 40  
r = about 1 to about 8

11. The system of claim 6, wherein the processor encrypts data by xoring data to be encrypted after a preselected number of iterations of the chaotic equations.

12. The encryption system of claim 6, wherein the protocol responsive memory further comprises:

- a. a memory partition for storing a read password;
- b. a comparator, connected to the memory partition and to the processor, for executing the protocol.

13. The system of claim 12, wherein the protocol comprises:

- 5
- a. a check password generated by the processor and transmitted to the comparator;
  - b. a comparison of the check password to the read password by the comparator;
  - c. transmission of the initial conditions by the protocol responsive memory to the processor if the comparison results in a match between the check password and the read



- 47 -

password.

14. The system of claim 6, wherein the protocol comprises:
- a. generation of an address by the processor;
  - b. transmission of the address by the processor to the protocol responsive memory; and
  - 5 c. transmission of the initial conditions by the protocol responsive memory to the processor upon receipt of the address by the protocol responsive memory.
15. The encryption system of Claim 6, further comprising:
- a. a memory connected to the processor to store and allow access to the iterated results of the initial conditions; and
  - b. the processor being further programmed to insert the iterated
  - 5 results of the initial conditions into the chaotic equations before iterating the chaotic equations.
16. An encryption system comprising:
- a. a first memory for holding data to be encrypted;
  - b. a second memory for holding encrypted data;
  - c. a slave processor having a memory for storage of initial
  - 5 conditions and a memory for storage of a password;
  - d. the slave processor programmed to release the initial conditions upon receipt of the password;

- 48 -

e. a master processor connected to the first and second memories and the slave processor, programmed to:

- (1) send the password to the slave processor;
- (2) store the initial conditions returned by the slave processor;
- (3) iteratively apply the initial conditions to equations of the following type:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x'$ ,  $y'$  and  $z'$  are iterated results of the equations given initial conditions  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$ , and  $b$ ;

- (4) read data from the first memory;
- (5) combine the data with the iterated results to create encrypted data; and
- (6) store the encrypted data in the second memory.

17. The encryption system of Claim 16, further comprising:

- a. a third memory connected to the processor for holding the iterated results of the equations; and
- b. the master processor being further programmed to insert the iterated results into the equations.

- 49 -

18. The encryption system of claim 16, wherein the initial conditions are in the range:

5         $x$  = about -30 to about 50, excluding 0  
        $y$  = about -30 to about 50, excluding 0  
        $z$  = about -30 to about 50, excluding 0  
        $\sigma$  = about .006 to about .028  
        $b$  = about 24 to about 40  
        $r$  = about 1 to about 8

19. The encryption system of claim 16, wherein the master processor is a member of the *Motorola 68000* family of microprocessors.

20. The encryption system of claim 16, wherein the master processor is a member of the *Intel Ix86* family of microprocessors.

21. The encryption system of claim 16, wherein the slave processor is the *Xicor x76041*.

22. The encryption system of claim 16, wherein the processor is programmed to iterate the equations a predetermined number of times before combining the data with the iterated results.

23. A data encryption system comprising:

- 5        a. a first memory for holding data to be encrypted;
- b. a second memory for holding encrypted data;
- c. a third memory for holding a master processor password;
- d. an input device;
- e. a slave processor having a memory for storage of a serial number, a read password and a set of initial conditions;

- 50 -

- 5
- f. the slave processor programmed to release the serial number when polled and to release the initial conditions only upon receipt of the read password;
- g. a master processor connected to the first, second and third memories and the input device and removably connected to the slave processor;
- h. the master processor programmed to:
- 10
- (1) poll the slave processor and store the serial number returned by the slave processor in temporary memory;
- (2) access the input device and store identification data input from the input device in temporary memory;
- (3) access the third memory, retrieve the master processor password and store the master processor password in temporary memory;
- 15
- (4) xor the serial number, the identification number and the master processor password and store the result in temporary memory as the read password;
- (5) transmit the read password to the slave processor;
- 20
- (6) read the initial conditions returned by the slave processor;

- 51 -

- (7) apply the initial conditions to a set of chaotic equations;
- (8) iterate the chaotic equations and store iterated results;
- (9) read the data to be encrypted from the first memory;
- 5 (10) xor the data to be encrypted with the iterated results and store the result.

24. The system of claim 23, wherein the chaotic equations are of the form:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

5 where  $x'$ ,  $y'$  and  $z'$  are numeric results and where  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $b$  and  $r$  are initial conditions.

25. The system of claim 23, wherein the initial conditions comprise one parameter from each of the following ranges:

5  $x$  = about -30 to about 50, excluding 0  
 $y$  = about -30 to about 50, excluding 0  
 $z$  = about -30 to about 50, excluding 0  
 $\sigma$  = about .006 to about .028  
 $b$  = about 24 to about 40  
 $r$  = about 1 to about 8

26. The system of claim 23, where the input device is a keyboard.
27. The system of claim 23, where the input device is a card reader.

- 52 -

28. The system of claim 23, where the input device identifies a physical trait of the user to be identified.

29. The system of claim 23, wherein the identification data is a personal identification number.

30. The system of claim 23, wherein the slave processor is a *XICOR x76041* password access security supervisor.

31. The system of claim 23, wherein the master processor is a member of the *Intel Ix86* family of microprocessors.

32. The system of claim 23, wherein the master process is a member of the *Motorola 68000* family of microprocessors.

33. The system of claim 23, wherein the master processor is further programmed to iterate the chaotic equations a preselected number of times before xoring the data to be encrypted with the iterated results.

34. The system of claim 23, wherein the master processor is further programmed to insert the stored iterated results into the chaotic equations before iterating the chaotic equations.

35. The system of Claim 23, further comprising:

- a. a nonvolatile memory means for storing the iterated results;  
and
- b. the master processor further programmed to:

- 53 -

- (1) poll the nonvolatile memory means and determine if iterated results have been stored there; and
- (2) insert the iterated results into the chaotic equations before iterating chaotic equations if iterated results have been found in the nonvolatile memory;

36. A method of encrypting data comprising of the steps of:

- a. selecting a set of parameters from a predetermined valid parameter space;
- b. inserting the parameters into the chaotic equations of the form:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$  and  $b$  are parameters and  $x'$ ,  $y'$  and  $z'$  are numeric results;

- c. iterating the chaotic equations to derive a  $x'$  iterate stream, a  $y'$  iterate and a  $z'$  iterate stream;
- d. using the iterate streams to create a cipher stream; and
- e. encrypting data by combining the cipher stream with the data.

- 54 -

37. The method of claim 36, further comprising the step of:
- a. iterating the chaotic equations a predetermined number of times before creating the cipher stream.
38. The method of claim 36, further comprising the steps of:
- a. storing the numeric results; and
  - b. inserting the numeric results in the chaotic equations before iterating the chaotic equations.
39. The method of claim 36, wherein the step of selecting a set of parameters further comprises:
- a. selecting a set of parameters from the following valid parameter space:
- 5             $x = \text{about } -30 \text{ to about } 50, \text{ excluding } 0$   
               $y = \text{about } -30 \text{ to about } 50, \text{ excluding } 0$   
               $z = \text{about } -30 \text{ to about } 50, \text{ excluding } 0$   
               $\sigma = \text{about } .006 \text{ to about } .028$   
               $b = \text{about } 24 \text{ to about } 40$   
               $r = \text{about } 1 \text{ to about } 8$
40. A method of encrypting data comprising the steps of:
- a. selecting a set of parameters from a predetermined seed space;
  - b. inserting the parameters into chaotic equations of the form:

$$\begin{aligned} x' &= -\sigma x + \sigma y \\ y' &= rx - y - xz \\ z' &= bz + xy \end{aligned}$$



- 55 -

where  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $b$  and  $r$  are parameters and  $x'$ ,  $y'$  and  $z'$  are numeric results;

- 5
- c. iterating the chaotic equations to derive are  $x'$  iterate stream, a  $y'$  iterate stream and a  $z'$  iterate stream;
  - d. xoring the  $x'$  iterate stream, the  $y'$  iterate stream and the  $z'$  iterate stream to obtain a cipher number;
  - e. xoring the cipher number with the data to create encrypted data.

41. The method of claim 40, further comprising the step of:

- a. iterating the chaotic equations a preselected number of times before xoring the cipher number with the data.

42. The method of claim 40, wherein the predetermined seed space further comprises one value from each of the following ranges:

- 5
- $x$  = about -30 to about 50, excluding 0
  - $y$  = about -30 to about 50, excluding 0
  - $z$  = about -30 to about 50, excluding 0
  - $\sigma$  = about .006 to about .028
  - $b$  = about 24 to about 40
  - $r$  = about 1 to about 8

43. The method of claim 40, further comprising the steps of:

- a. storing the numeric results; and
- b. inserting the numeric results into the chaotic equations before iterating the chaotic equations.

- 56 -

44. A data decryption system comprising:

- a. a predetermined set of valid initial conditions;
- b. a protocol responsive memory programmed to store and allow access to the initial conditions in response to a protocol;
- c. a processor connected to the protocol responsive memory, the processor programmed to:
  - (1) execute the protocol;
  - (2) receive and store the initial conditions returned by the protocol responsive memory;
  - (3) insert the initial conditions into and iterate a set of chaotic equations to arrive at iterated results; and
  - (4) create decrypted data by xoring the data with the iterated results.

45. The data decryption system of Claim 44, further comprising a transmitter connected to the processor for transmitting the decrypted data.

46. The data decryption system of Claim 44, further comprising a second memory connected to the processor to store the decrypted data.

- 57 -

47. The system of Claim 44, wherein the set of chaotic equations are of the form:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x'$ ,  $y'$  and  $z'$  are iterated results of initial conditions  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$ , and  $b$ .

48. The system of Claim 44, wherein the predetermined valid initial conditions are in the range:

5  
 $x$  = about -30 to about 50, excluding 0  
 $y$  = about -30 to about 50, excluding 0  
 $z$  = about -30 to about 50, excluding 0  
 $\sigma$  = about .006 to about .028  
 $b$  = about 24 to about 40  
 $r$  = about 1 to about 8

49. A system comprising:

- 5
- a. a first memory for holding data to be decrypted;
  - b. a second memory for holding decrypted data;
  - c. a slave processor having a memory for storage of initial conditions and a memory storage of a password;
  - d. the slave processor programmed to release the initial conditions upon receipt of the password;

- 58 -

e. a master processor connected to the first and second memories and the slave processor, programmed to:

- (1) send the password to the slave processor;
- (2) store the initial conditions returned by the slave processor;
- (3) iteratively apply the initial conditions to equations of the following type:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x'$ ,  $y'$  and  $z'$  are iterated results of the equations given initial conditions  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$ , and  $b$ ;

- (4) read data from the first memory;
- (5) combine the data with the iterated results to create decrypted data; and
- (6) store the decrypted data in the second memory.

50. The system of claim 49, wherein the processor is programmed to iterate the equations a predetermined number of times before combining the data with the iterated results.

- 59 -

51. The system of claim 49, wherein the processor is programmed to iterate the equations a predetermined number of time before xoring the data with the iterate results.

52. A data decryption system comprising:

- a. a first memory for holding data to be decrypted;
- b. a second memory for holding decrypted data;
- c. a third memory for holding a master processor password;
- 5 d. an input device;
- e. a slave processor having a memory for storage of a serial number, a read password and a set of initial conditions;
- f. the slave processor programmed to release the serial number when polled and to release the initial conditions only upon receipt of the read password;
- 10 g. a master processor connected to the first, second and third memories and the input device and removably connected to the slave processor;
- h. the master processor programmed to:
  - 15 (1) poll the slave processor and store the serial number returned by the slave processor in temporary memory;

- 60 -

- (2) access the input device and store identification data  
input from the input device in temporary memory;
- (3) access the third memory, retrieve the master  
processor password and store the master processor  
password in temporary memory;
- (4) xor the serial number, the identification number and  
the master processor password and store the result in  
temporary memory as the read password;
- (5) transmit the read password to the slave processor;
- (6) read the initial conditions returned by the slave  
processor;
- (7) apply the initial conditions to a set of chaotic  
equations;
- (8) iterate the chaotic equations and store iterated results;
- (9) read the data to be decrypted from the first memory;
- (10) xor the data to be decrypted with the iterated results  
and store the results.

- 61 -

53. The system of claim 52, wherein the chaotic equations are of the form:

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= r s - y - x z \\z' &= b z + x y\end{aligned}$$

where  $x'$ ,  $y'$  and  $z'$  are numeric results and where  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $b$  and  $r$  are initial conditions.

54. The system of claim 52, wherein the initial conditions comprise one parameter from each of the following ranges:

5  $x$  = about -30 to about 50, excluding 0  
 $y$  = about -30 to about 50, excluding 0  
 $z$  = about -30 to about 50, excluding 0  
 $\sigma$  = about .006 to about .028  
 $b$  = about 24 to about 40  
 $r$  = about 1 to about 8

55. The system of claim 52, wherein the master processor is further programmed to iterate the chaotic equations a preselected number of times before xoring the data to be decrypted with the iterated results.

56. A method of decrypting data comprising of the steps of:

- a. selecting a set of parameters from a predetermined valid parameter space;
- b. inserting the parameters into the chaotic equations of the form:
- 5

- 62 -

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $r$  and  $b$  are parameters and  $x'$ ,  $y'$  and  $z'$  are numeric results;

- 5           c.     iterating the chaotic equations to derive a  $x'$  iterate stream, a  $y'$  iterate and a  $z'$  iterate stream;
- d.     using the iterate streams to create a cipher stream; and
- e.     decrypting data by combining the cipher stream with the data.

57.     The method of claim 56, further comprising the step of iterating the chaotic equation a predetermined number of times before creating the cipher stream.

58.     The method of claim 56, wherein the step of selecting a set of parameters further comprises:

- a.     selecting a set of parameters from the following valid parameter space:

- 5            $x$  = about -30 to about 50, excluding 0  
               $y$  = about -30 to about 50, excluding 0  
               $z$  = about -30 to about 50, excluding 0  
               $\sigma$  = about .006 to about .028  
               $b$  = about 24 to about 40  
               $r$  = about 1 to about 8



- 63 -

59. A method of encrypting and decrypting data comprising the steps of:

- a. selecting a set of parameters from a predetermined seed space;
- b. inserting the parameters into chaotic equations of the form:

5

$$\begin{aligned}x' &= -\sigma x + \sigma y \\y' &= rs - y - xz \\z' &= bz + xy\end{aligned}$$

where  $x$ ,  $y$ ,  $z$ ,  $\sigma$ ,  $b$  and  $r$  are parameters and  $x'$ ,  $y'$  and  $z'$  are numeric results;

10

- c. iterating the chaotic equations to derive are  $x'$  iterate stream, a  $y'$  iterate stream and a  $z'$  iterate stream;
- d. xoring the  $x'$  iterate stream, the  $y'$  iterate stream and the  $z'$  iterate stream to obtain a cipher number;
- e. encrypting data by xoring the cipher number with the unencrypted data; and
- f. decrypting data by xoring the cipher number with the encrypted data.

60. The method of claim 59, further comprising the step of:

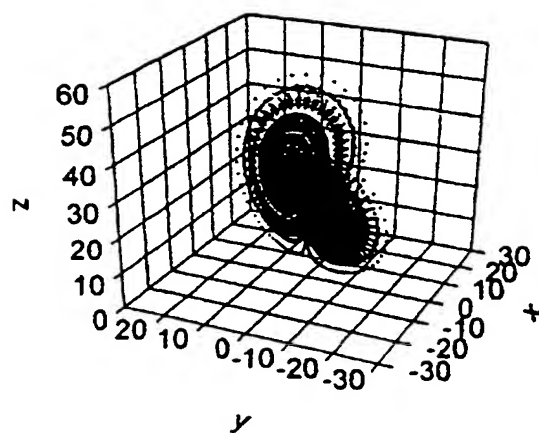
- a. iterating the number of times before xoring the cipher number with the data.

- 64 -

61. The method of claim 59, wherein the predetermined seed space further comprises one value from each of the following ranges:

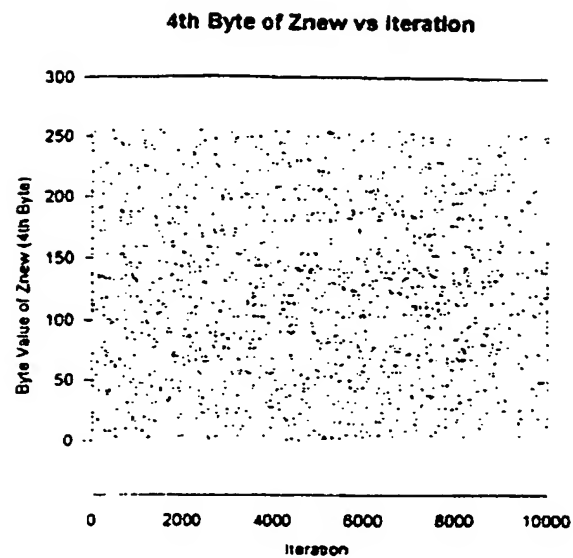
5         $x$  = about -30 to about 50, excluding 0  
        $y$  = about -30 to about 50, excluding 0  
        $z$  = about -30 to about 50, excluding 0  
        $\sigma$  = about .006 to about .028  
        $b$  = about 24 to about 40  
        $r$  = about 1 to about 8

1/16



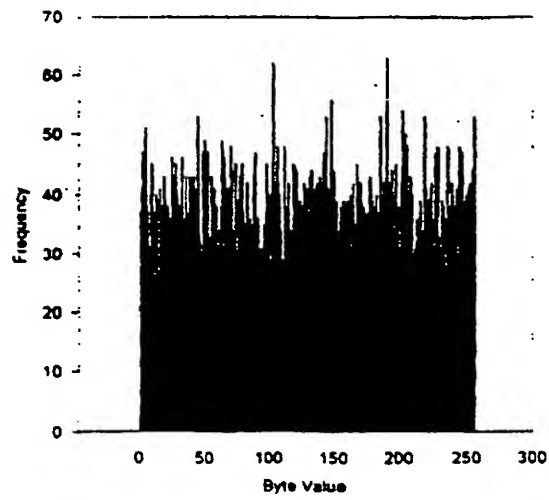
$X_0 = 0, Y_0 = 2, Z_0 = 23$   
 $\sigma = .01, r = 28, b = 8.3$

2/16



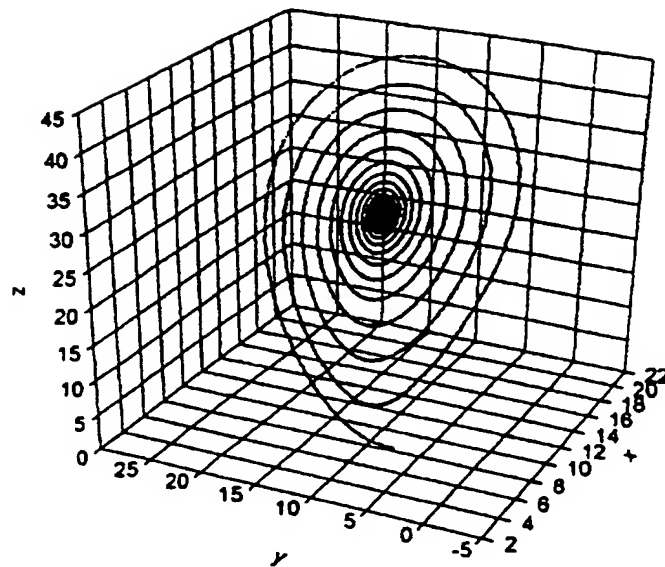
3/16

Histogram of 4th byte of z stream



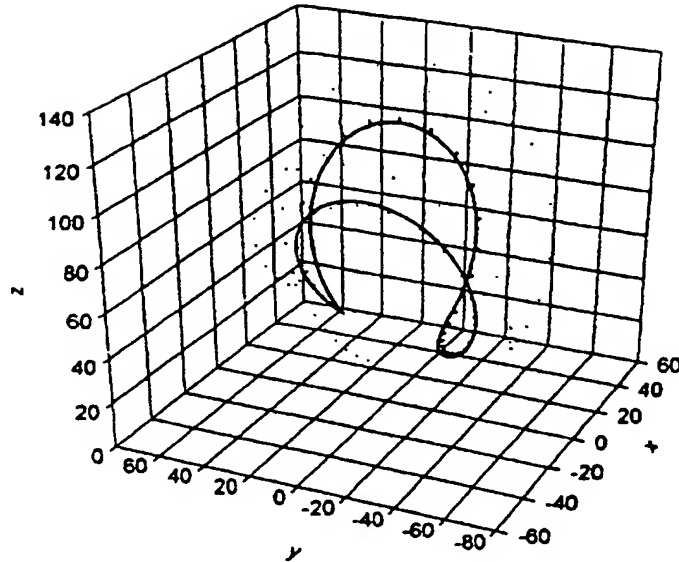
4/16

$X_0 = Y_0 = Z_0 = 5$   
 $\sigma = .001, r = 28, b = 6$



5/16

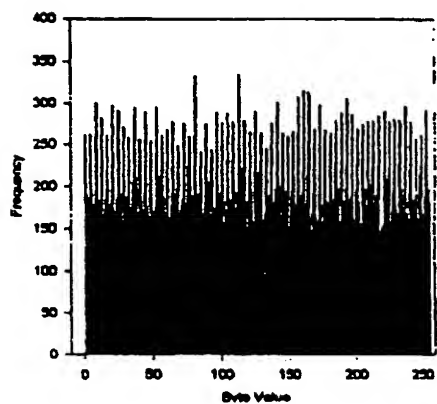
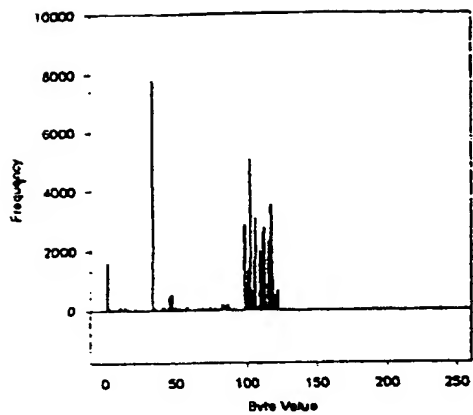
$X_0 = Y_0 = Z_0 = 10$   
 $\sigma = .01, r = 60, b = 6.7$



6/16

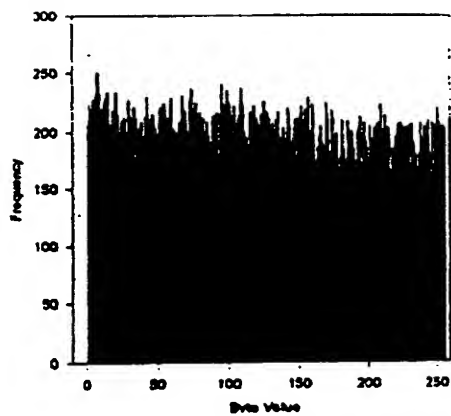
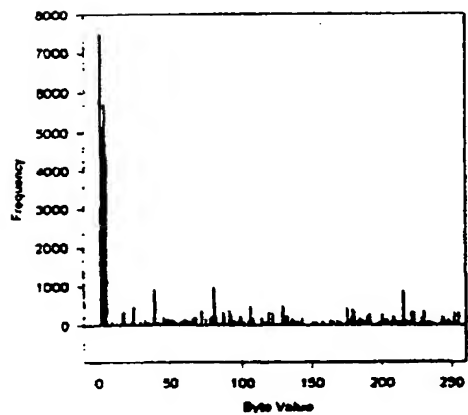
6A

6b



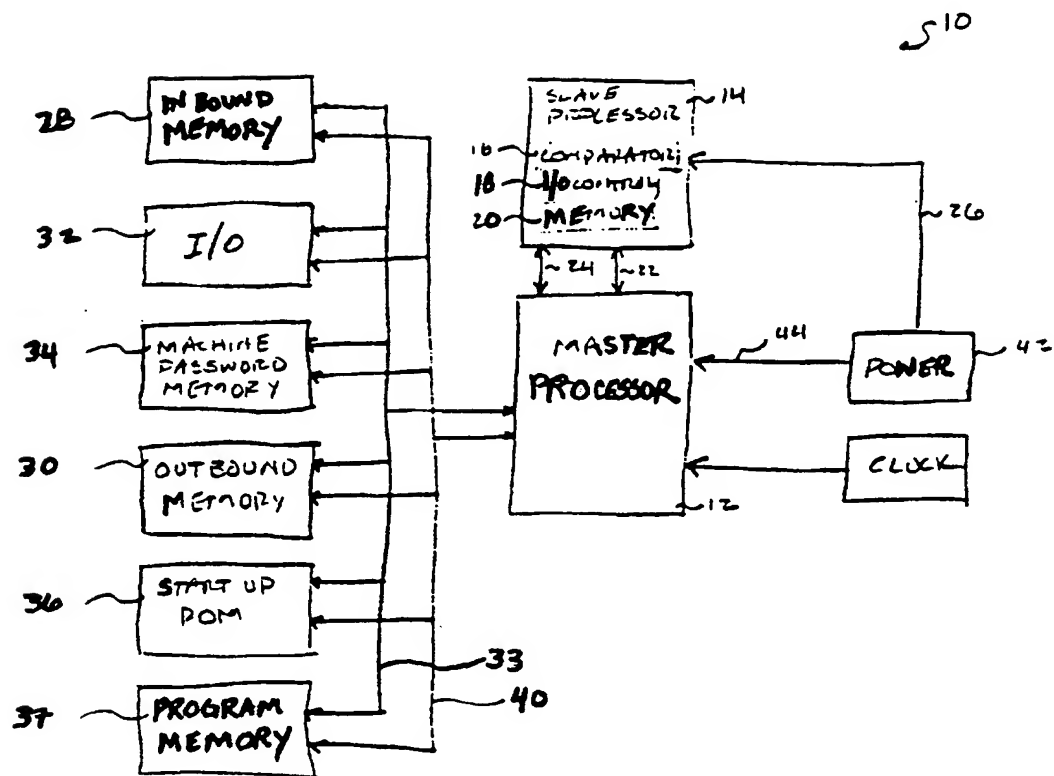
6c of 16

6d of 16

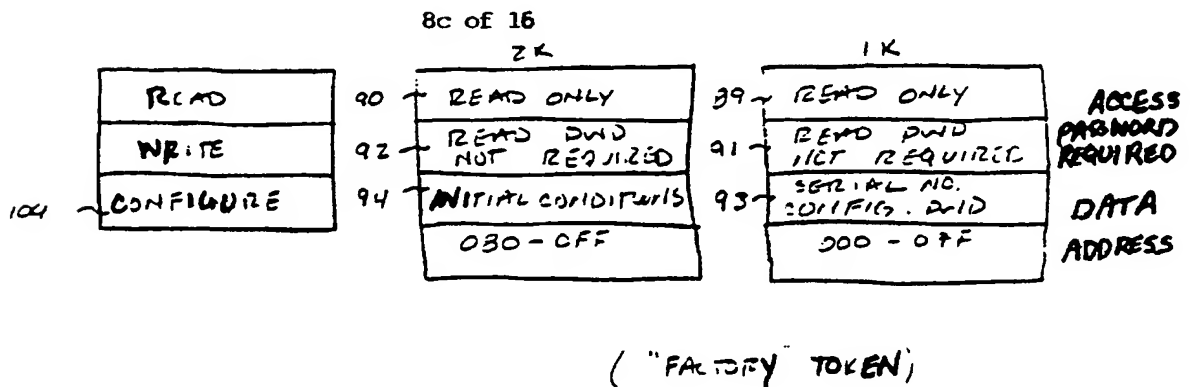
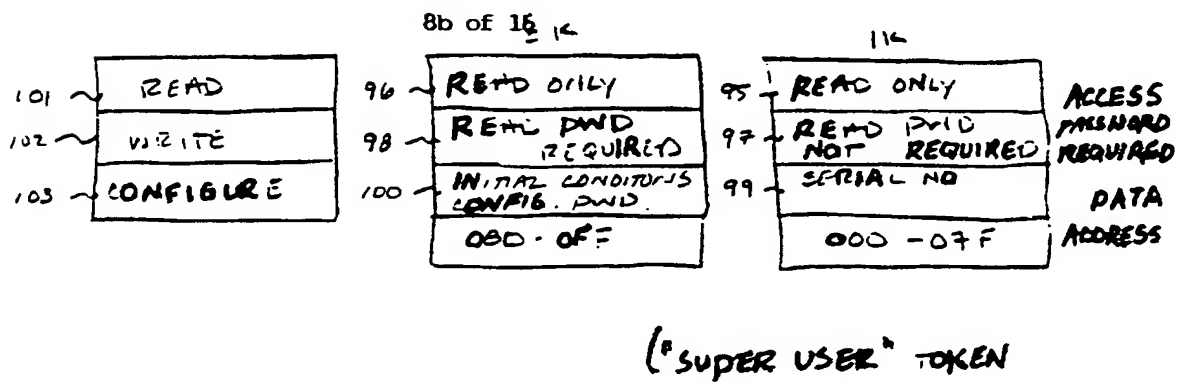
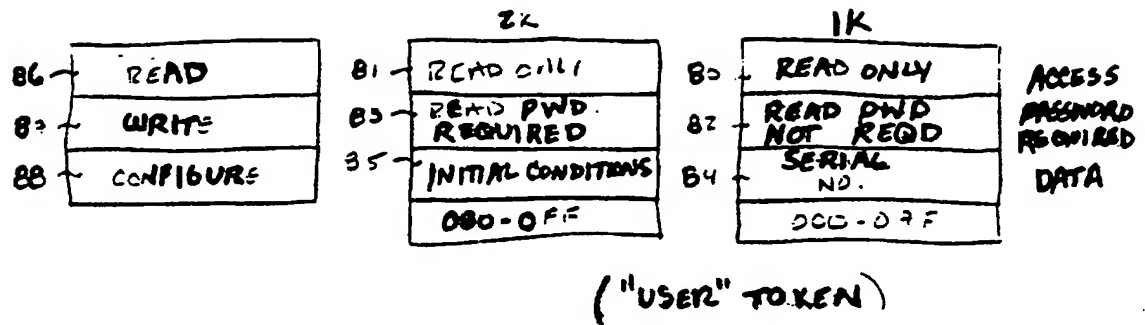




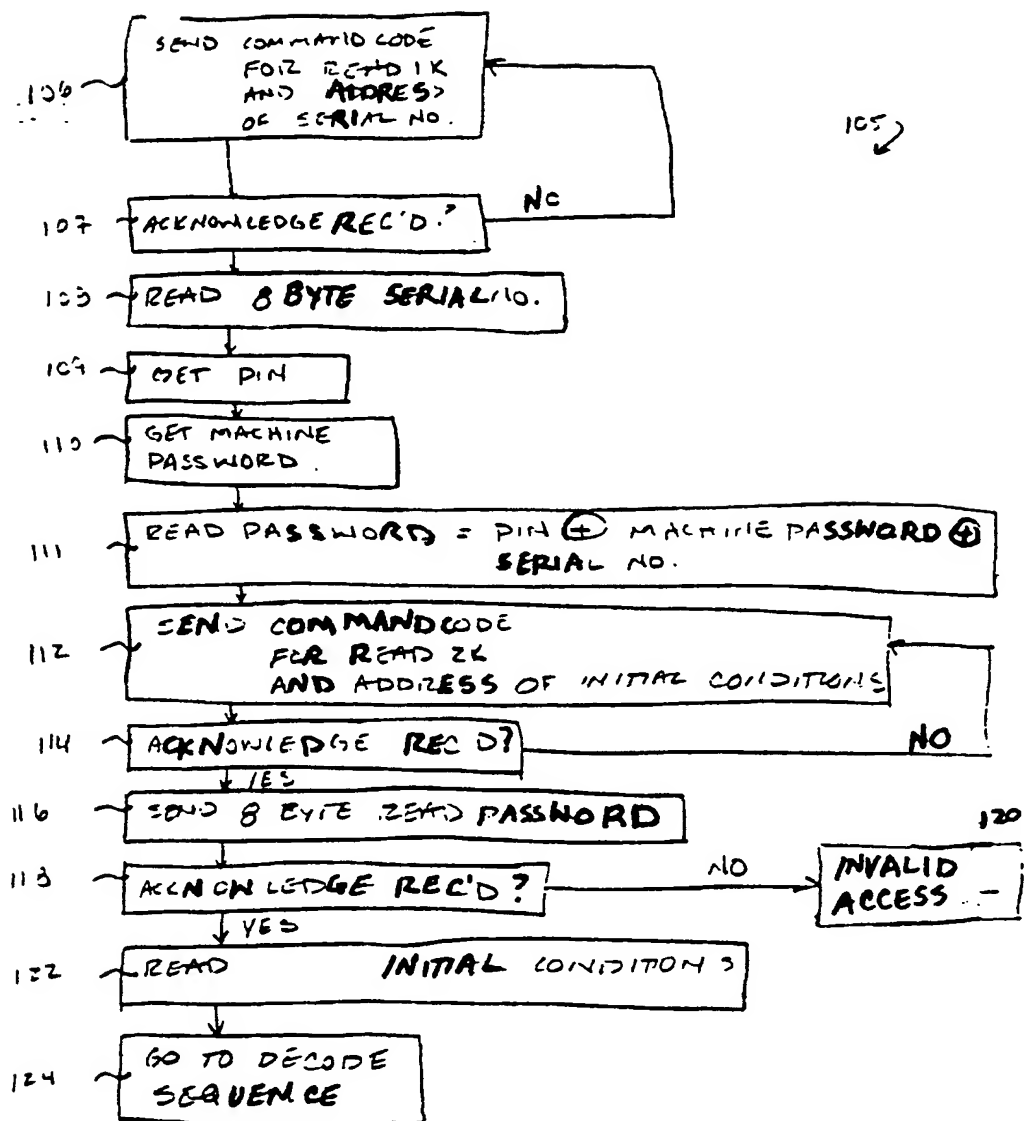
7/16



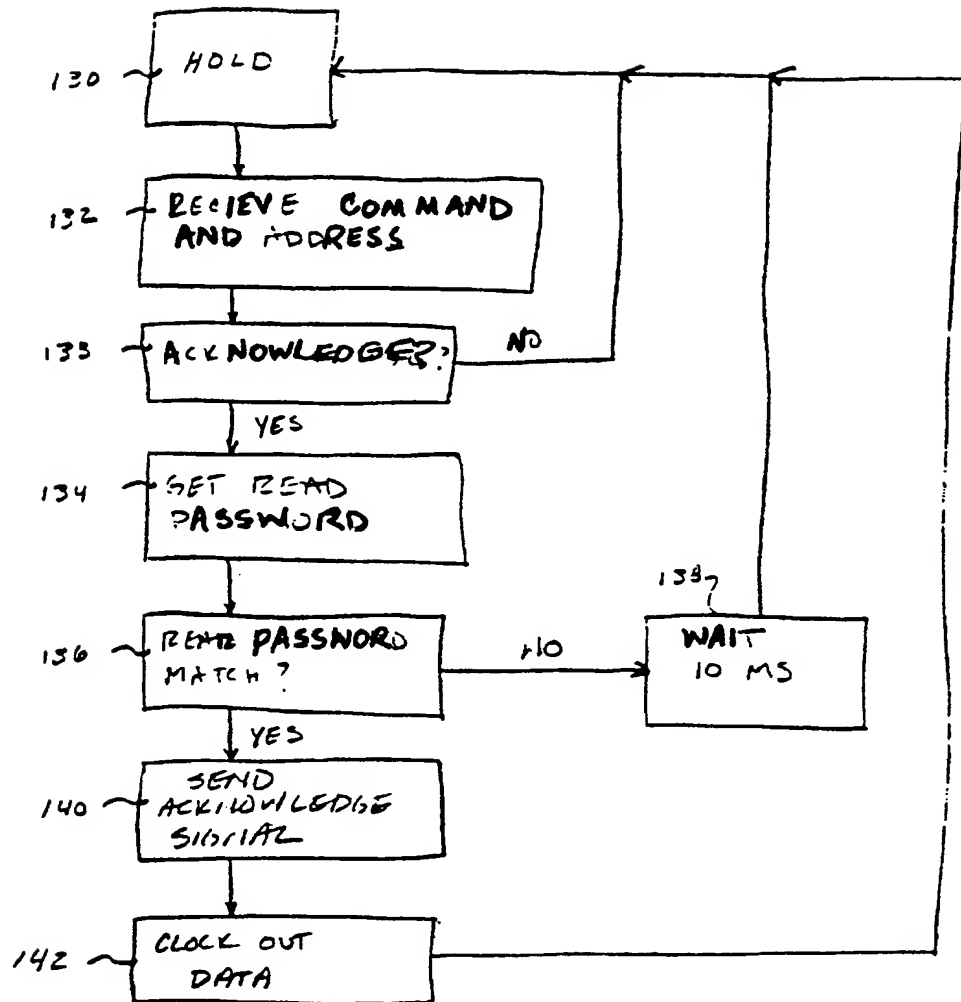
8/16



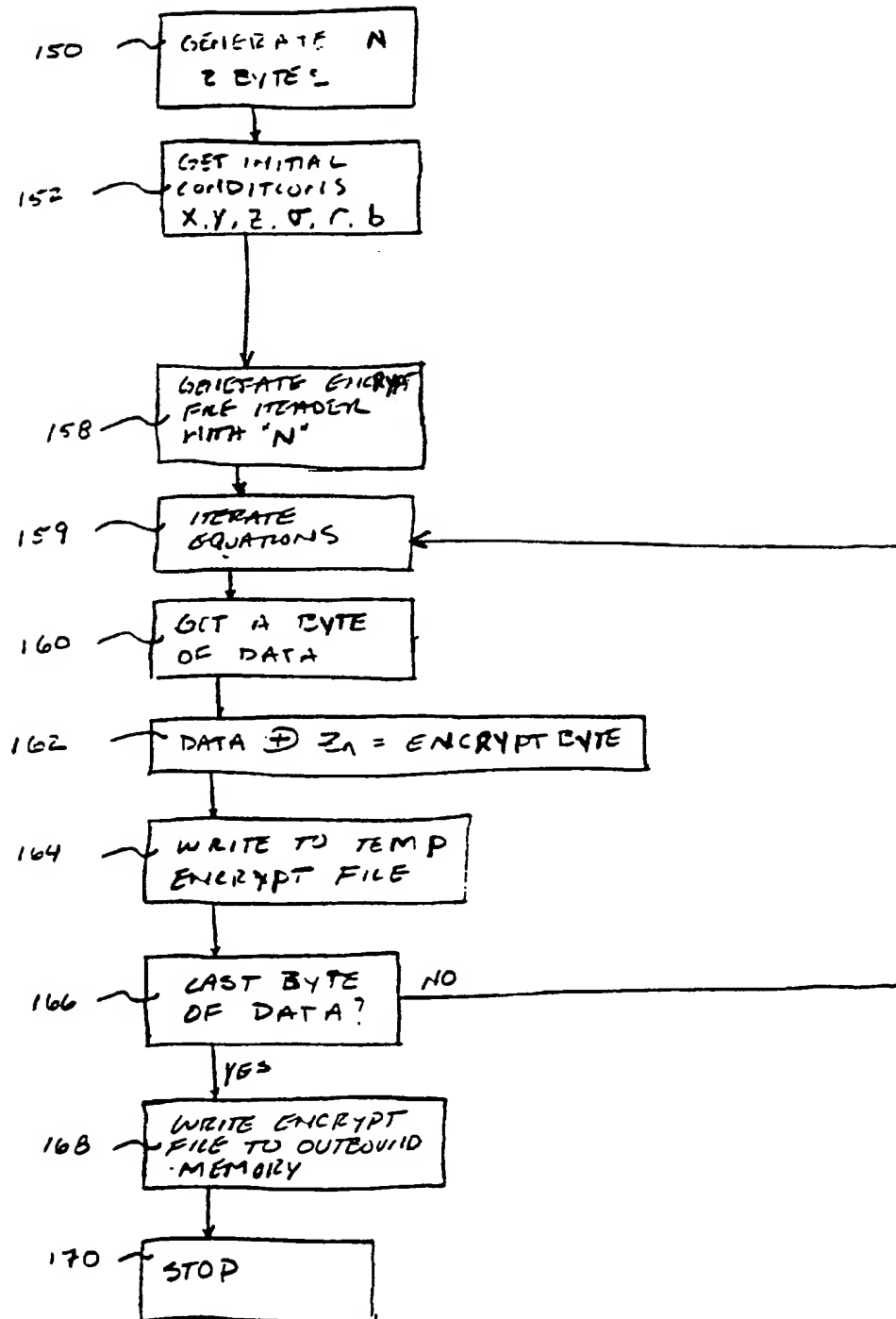
9/16



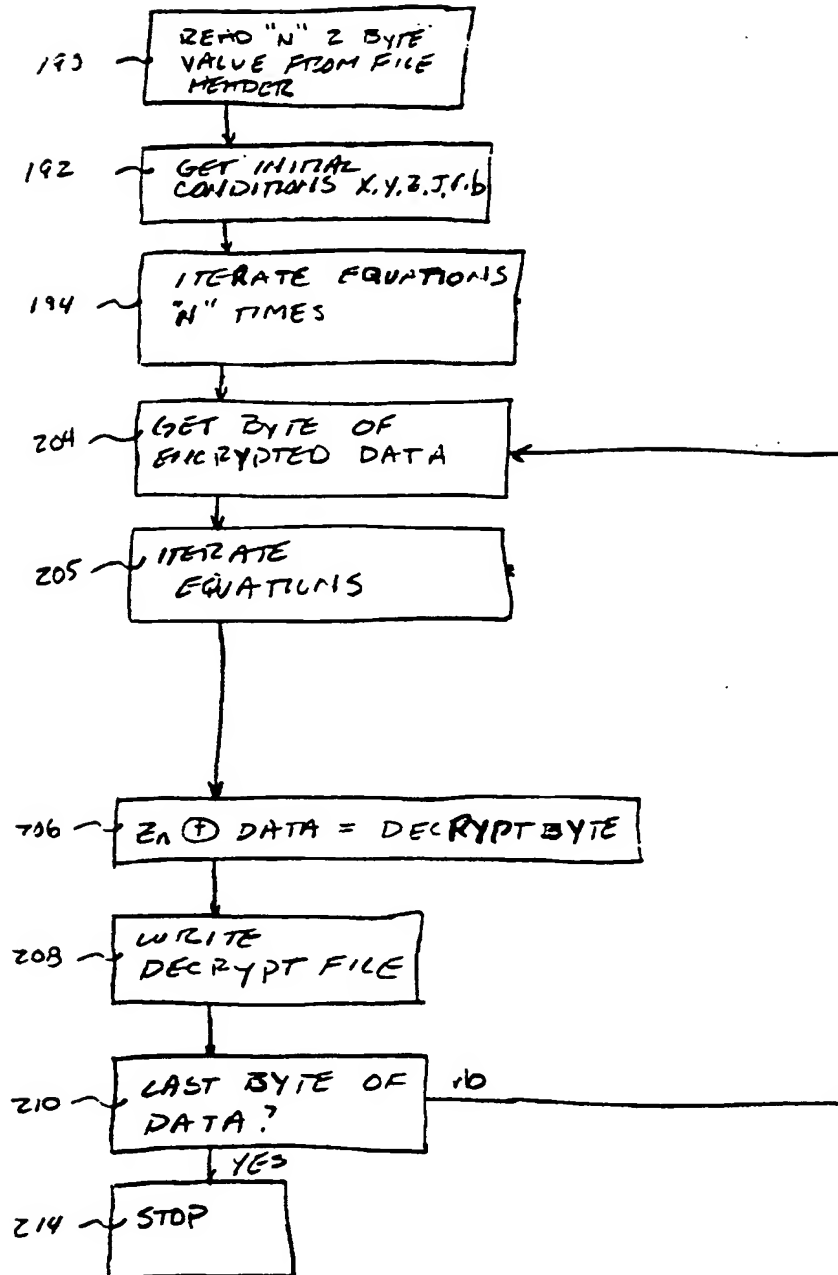
10/16



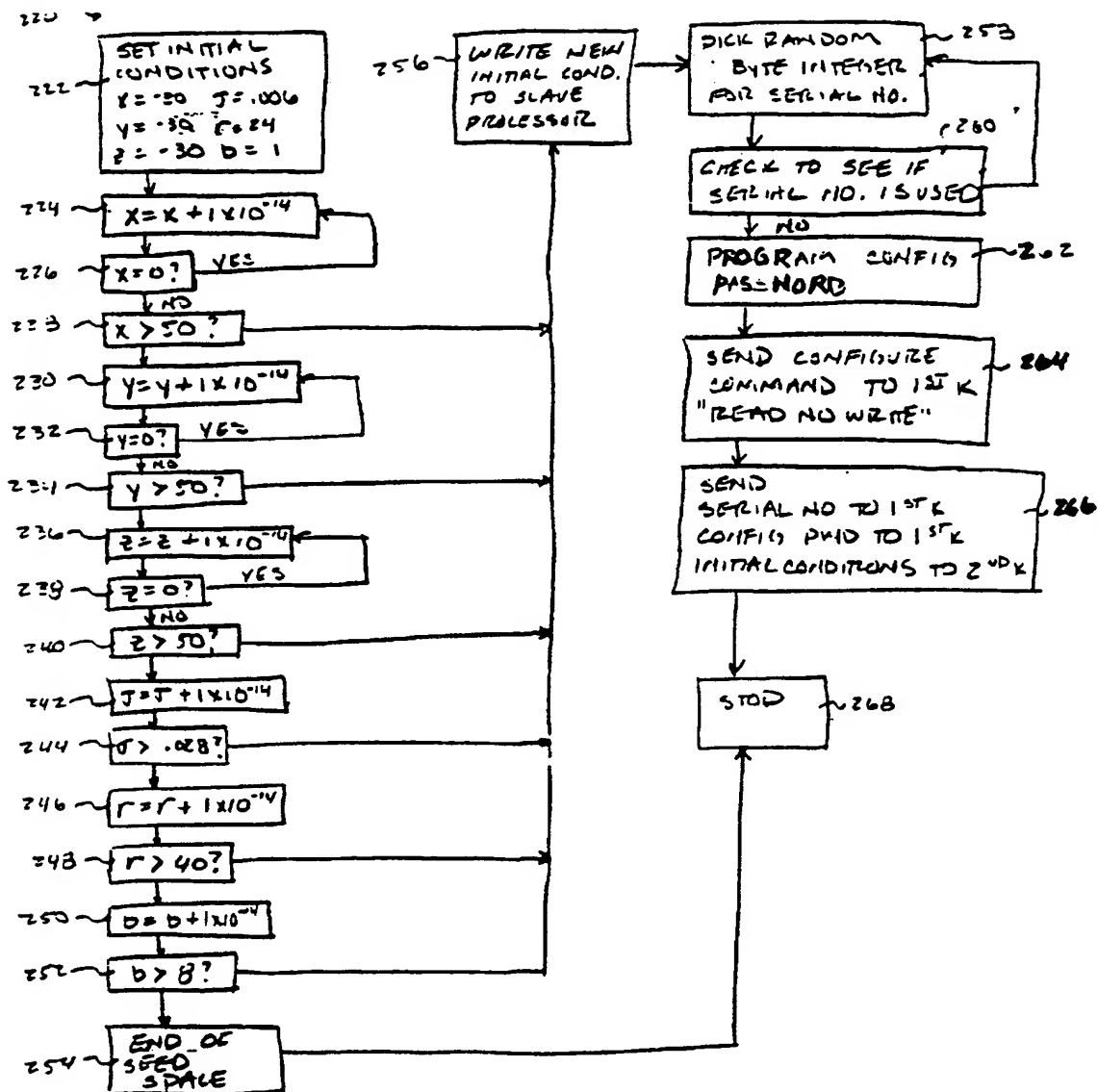
11/16



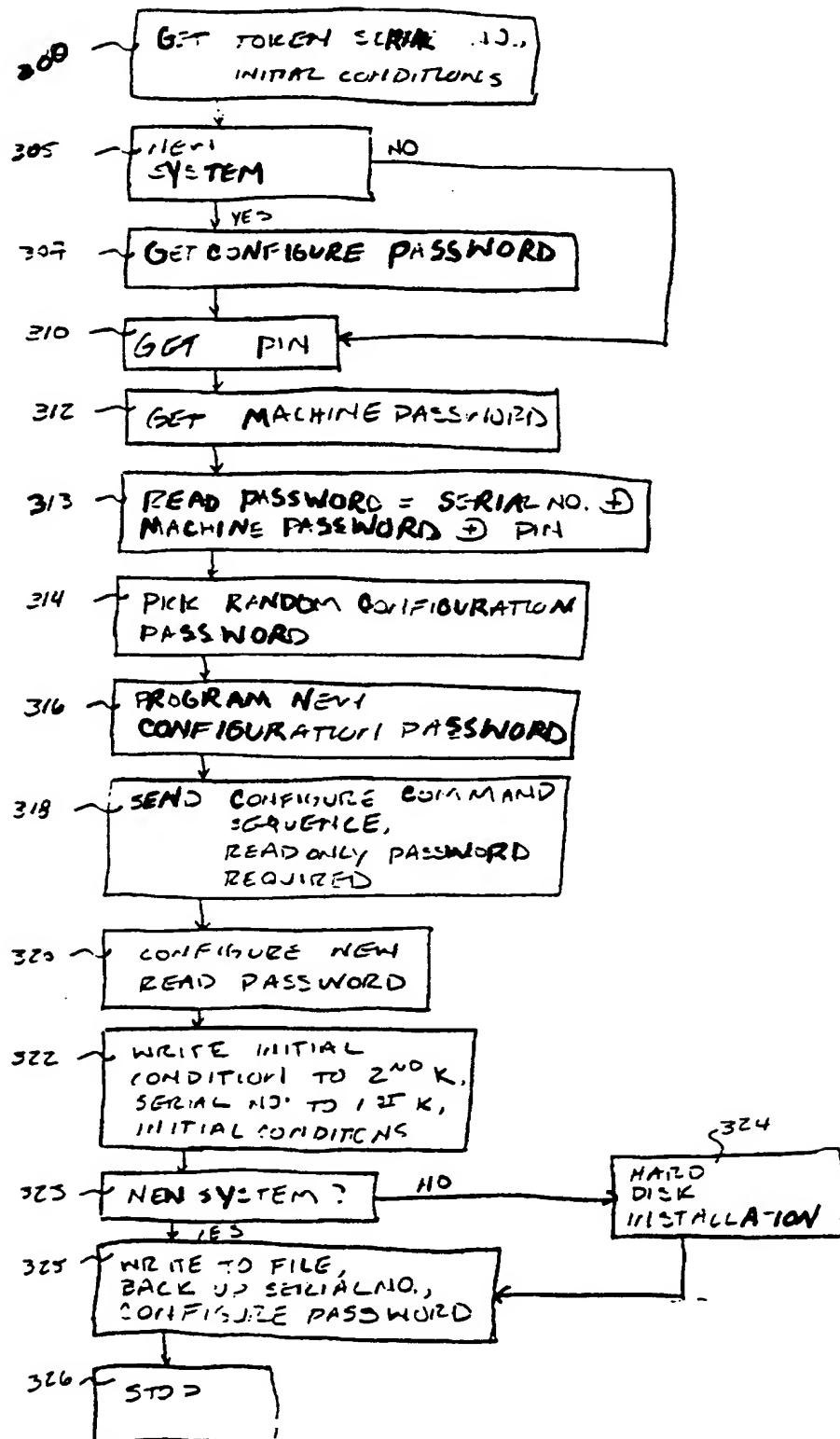
12/16



13/16

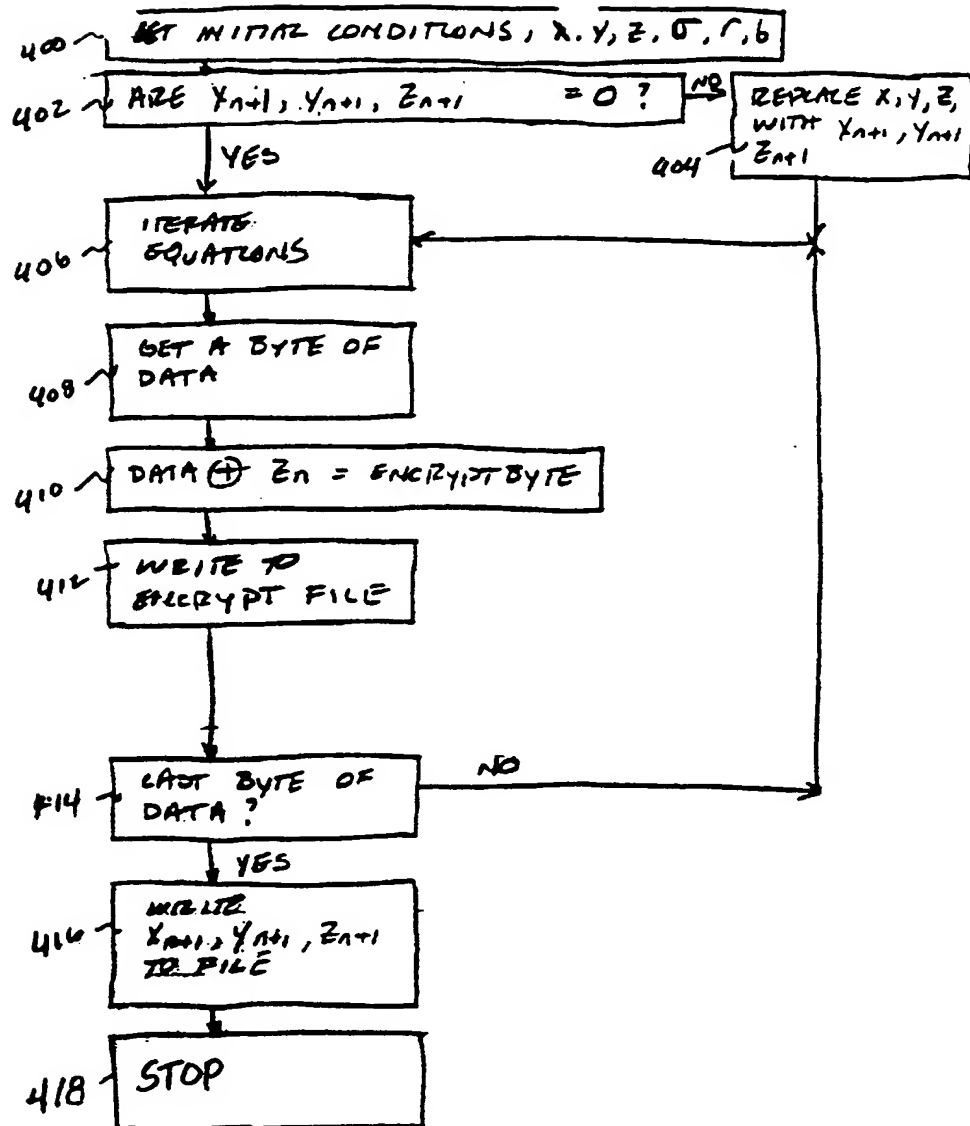


14/16

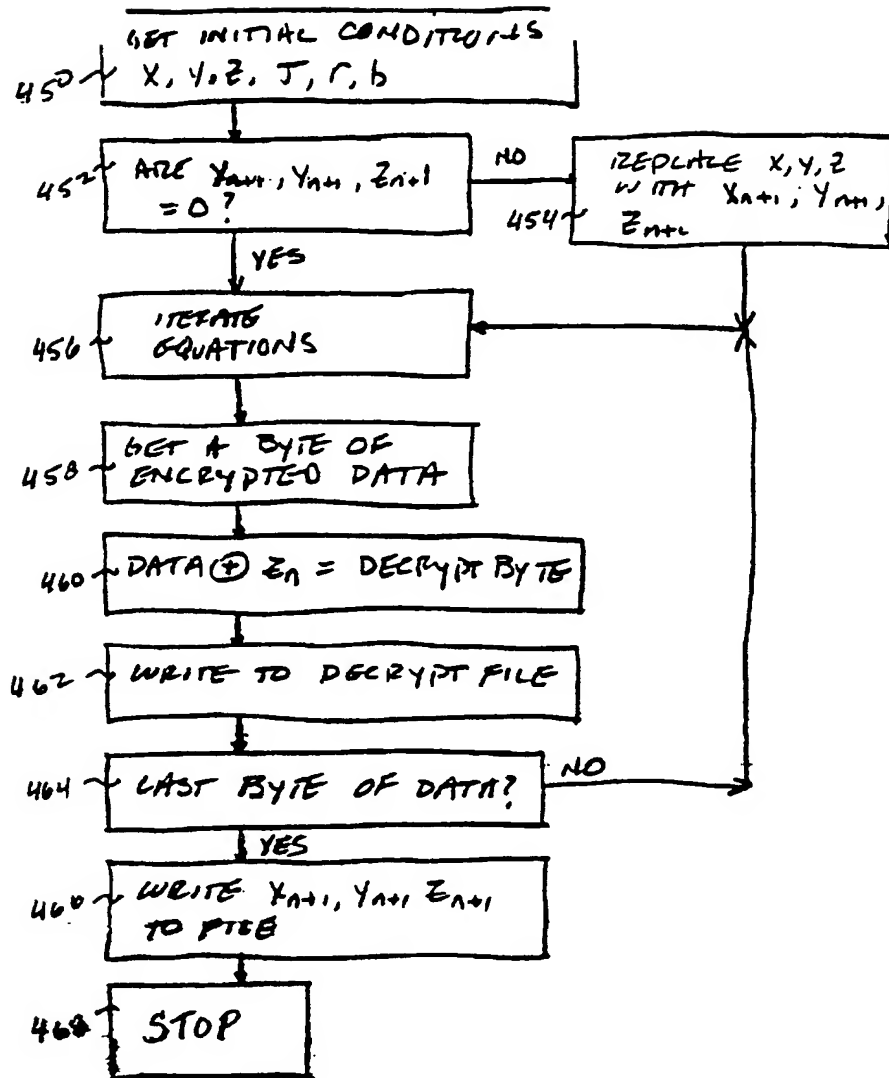




15/16



16/16



# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US97/15869

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(6) :H04L 9/28 US CL :380/28, 46; 364/717.01 According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) U.S. : 380/28, 46, 48; 364/717.01, 717.05 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) INTERNET, APS terms: chaotic equations, chaotic systems, chaotic dynamics, dynamic systems, lorenz		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,291,555 A (CUOMO et al.) 01 March 1994, see entire document.	6, 7, 9, 11, 36-38, 56, 57
X	US 5,432,697 A (HAYES) 11 July 1995, see entire document.	1, 2, 6-11, 36-48, and 56-61
X	US 5,048,086 A (BIANCO et al.) 10 September 1991, see entire document.	6, 7, 11, 44, and 45
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "B" earlier document published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "A" document member of the same patent family		
Date of the actual completion of the international search 24 NOVEMBER 1997		Date of mailing of the international search report 14 JAN 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer <i>Pinchus M. Laufer</i> PINCHUS M. LAUFER Telephone No. (703) 306-4177

**BLANK PAGE**